



**SANS Technology  
Institute**

11200 Rockville Pike, Ste. 200  
North Bethesda, MD, 20851  
(301) 241-7665 | info@sans.edu

ALAN PALLER  
*President*

DAVID HOELZER  
*Dean of Faculty*

JOHANNES ULLRICH, Ph.D.  
*Dean of Research*

TIM MEDIN  
*MSISE Program Director*

ERIC PATTERSON  
*Executive Director*

BETSY MARCHANT  
*Assistant Director,  
School Operations*

May 22, 2020

James D. Fielder, Jr., Ph.D.  
Secretary of Higher Education  
Maryland Higher Education Commission  
Nancy S. Grasmick Building, 10<sup>th</sup> floor  
6 North Liberty St.  
Baltimore, MD 21201

Dear Dr. Fielder,

It is with great enthusiasm that the SANS Technology Institute submits the attached proposal to create a Bachelor of Professional Studies degree in Applied Cybersecurity.

We believe that this program will provide talented Maryland students with a smooth, assured pathway to high-paying jobs in critical technical roles in cybersecurity. Even before the program has been launched, 13 Maryland employers as well as employers from outside the state have expressed an interest in interviewing the students who master the material covered in this program and demonstrate that mastery by earning five Global Information Assurance Certifications (GIAC).

I look forward to answering any questions you or your staff may have or providing additional information as needed. I can be reached by cell phone at 301-520-2835.

Sincerely,

A handwritten signature in blue ink, appearing to read "Alan Paller", with a large, looping flourish at the end.

Alan Paller  
President  
SANS Technology Institute



## Cover Sheet for In-State Institutions

### New Program or Substantial Modification to Existing Program

Institution Submitting Proposal	SANS Technology Institute
---------------------------------	---------------------------


*Each action below requires a separate proposal and cover sheet.*

- |   |   |
|---|---|
| <input checked="" type="radio"/> New Academic Program | <input type="radio"/> Substantial Change to a Degree Program            |
| <input type="radio"/> New Area of Concentration       | <input type="radio"/> Substantial Change to an Area of Concentration    |
| <input type="radio"/> New Degree Level Approval       | <input type="radio"/> Substantial Change to a Certificate Program       |
| <input type="radio"/> New Stand-Alone Certificate     | <input type="radio"/> Cooperative Degree Program                        |
| <input type="radio"/> Off Campus Program              | <input type="radio"/> Offer Program at Regional Higher Education Center |

Payment <input type="radio"/> Yes Submitted: <input checked="" type="radio"/> No	Payment <input type="radio"/> R*STARS Type: <input type="radio"/> Check	Payment Amount:	Date Submitted:
---	--	--------------------	--------------------

Department Proposing Program	SANS Technology Institute		
Degree Level and Degree Type	Bachelor of Professional Studies		
Title of Proposed Program	Bachelor of Professional Studies in Applied Cybersecurity		
Total Number of Credits	120		
Suggested Codes	HEGIS: 5199		CIP: 11 1003
Program Modality	<input checked="" type="radio"/> On-campus		<input type="radio"/> Distance Education ( <i>fully online</i> )
Program Resources	<input checked="" type="radio"/> Using Existing Resources		<input type="radio"/> Requiring New Resources
Projected Implementation Date	<input checked="" type="radio"/> Fall	<input type="radio"/> Spring	<input type="radio"/> Summer      Year: 2020
Provide Link to Most Recent Academic Catalog	URL: <a href="https://www.sans.edu/downloads/STI-2019-Undergraduate">https://www.sans.edu/downloads/STI-2019-Undergraduate</a>		

Preferred Contact for this Proposal	Name: Eric Patterson
	Title: Executive Director
	Phone: (440) 321-3040
	Email: <a href="mailto:epatterson@sans.edu">epatterson@sans.edu</a>

President/Chief Executive	Type Name: Alan Paller
	Signature:  Date: 22 May 2020
	Date of Approval/Endorsement by Governing Board: 22 May 2020

Revised 4/2020

PROPOSAL FOR A  
BACHELOR OF PROFESSIONAL STUDIES IN  
APPLIED CYBERSECURITY

SANS Technology Institute

## Table of Contents

A. Centrality to Institutional Mission Statement and Planning Priorities 1 .....	4
1. Program Description .....	4
2. Relation to the Mission and Strategic Goals of the SANS Technology Institute .....	5
3. Funding for the Program .....	5
4. STI's Commitment to the Long-Term Success of the Program .....	6
B. Critical and Compelling Regional and Statewide Need as Identified in the State Plan .....	6
1a. Critical Need for the BACS Program .....	6
1b. The Key Benefit of BACS .....	7
2. Alignment with the 2017–2021 Maryland State Plan .....	8
C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State .....	10
1. Market Demand for Cybersecurity Professionals .....	10
2. Demand for BACS Graduates .....	11
3. Current and Projected Supply of Cybersecurity Graduates .....	13
D. Reasonableness of Program Duplication .....	15
1. Similarities and Differences between the BACS Program and Other Programs Awarding Bachelor's Degrees in Cybersecurity .....	15
2. Admissions Requirements .....	16
E. Relevance to High-Demand Programs at Historically Black Institutions (HBIs) .....	17
F. Relevance to the Identity of Historically Black Institutions (HBIs) .....	17
G. Adequacy of Curriculum Design and Delivery to Related Learning Outcomes .....	17
1. Describe how the proposed program was established, and the faculty .....	17
2. Describe educational objectives and learning outcome .....	18
3. Explain how the institution will:	
a) provide for assessment of student achievement of learning outcomes .....	20
b) document student achievement of learning outcomes in the program .....	20
4. Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements .....	22
5. Discuss how general education requirements will be met, if applicable .....	36
6. Identify any specialized accreditation or graduate certification requirements for this program and its students .....	36
7. If contracting with another institution or non-collegiate organization, provide a copy of the written contract .....	36
8. Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information on the program ....	37
9. Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available .....	37

H. Adequacy of Articulation.....	38
I. Adequacy of Financial Resources with Documentation (outlined in COMAR 13B.02.03.14) .....	38
J. Adequacy of Library Resources (outlined in COMAR 13B.02.03.12).....	42
K. Adequacy of Physical Facilities, Infrastructure, and Instructional Equipment.....	43
L. Adequacy of Financial Resources with Documentation (outlined in COMAR 13B.02.03.14) .....	44
M. Adequacy of Provisions for Evaluation of the Program (outlined in COMAR 13B.02.03.15) .....	48
N. Consistency with the State’s Minority Student Achievement Goals (outlined in COMAR 13B.02.03.05 and in the State Plan for Postsecondary Education).....	49
O. Relationship to Low-productivity Programs Identified by the Commission .....	49
P. If Proposing a Distance Education Program, Please Provide Evidence of the Principles of Good Practice (outlined in COMAR 13B.02.03.22C).....	49
Appendix 1. Letters from Employers Ready to Interview and Hire Students Who Complete the Courses and Certifications of the BACS Program.....	50
Appendix 2. Contracts with Related Entities .....	64
Appendix 3. Evidence of Compliance with the Principles of Good Practice (outlined in COMAR 13B02.03.22C).....	79

## **A. Centrality to Institutional Mission Statement and Planning Priorities**

### **1. Program Description**

The SANS Technology Institute (STI) proposes to launch a Bachelor of Professional Studies in Applied Cybersecurity (“BACS”) program. BACS is designed to enable community college graduates who have completed an AAS degree with a GPA of 3.0 or greater to earn a bachelor’s degree. The degree will position students to win highly paid cybersecurity jobs immediately upon graduation. Under the BACS program, students will complete 70 credit hours at community colleges and 50 credit hours at STI where they will earn (as a requirement for graduation) at least five challenging and widely-sought-after professional cybersecurity certifications relied upon by U.S. law enforcement, intelligence services, and military organizations, large corporations, and contractors to validate the competencies of their full-time cybersecurity practitioners. BACS students will also develop and demonstrate proficiency in the fundamental technologies and skills that serve as the baseline for all professionals in cybersecurity, as well as mastery of effective written and oral communication of cybersecurity threats, vulnerabilities, and proposed improvements. The BACS program was designed in cooperation with Montgomery College in order to maximize the opportunity for community college students in Maryland to plan and complete a full four-year experience, maximizing the use of low-cost, accessible community college courses and leading to the BACS degree from the SANS Technology Institute.

BACS graduates will also have completed advanced cybersecurity coursework that will facilitate their hands-on mastery of one of the areas of specialization of greatest need in industry. The BACS specializations include security monitoring and detection, security operations, network vulnerability testing, web application testing, system and network forensics, and industrial control systems security. Students will also complete the corresponding nationally-recognized certification examination in their area of specialization. They will also complete an internship in which they use what they have learned while working inside organizations that operate large scale cybersecurity monitoring programs. Their preparation in BACS will set them apart from other cybersecurity bachelor’s degree holders because BACS graduates will already have completed the training and certifications that thousands of employers have previously had to pay for after they have hired new cybersecurity employees. Thus, BACS graduates will be among the most job-ready candidates for employers to consider hiring. To reinforce the attractiveness of BACS graduates to employers, the program also includes courses in the professional competencies that employers value highly: effective cybersecurity writing and presentations.

The proposed program will be delivered using the same live classroom settings, online modalities, and student management systems that are currently employed in delivering STI’s Master of Science in Information Security Engineering program and upper division certificate programs.

STI will employ a selection process for the BACS program designed to maximize the prospects that each BACS student will excel in his or her courses and become a highly-valued, elite cybersecurity professional. Towards that end, candidates for acceptance into the BACS program will be assessed using two robust evaluation tools. First, each candidate will complete the SANS

Cyber Talent Enhanced (CTE) exam, which gained national prominence when it was used by the U.S. Office of Management and Budget (OMB) to select students for the Federal Cybersecurity Reskilling Academy. The CTE allowed OMB to select 22 Reskilling Academy students from among 1,700 applicants who had no background in information technology or cybersecurity. Twenty of those 22 students excelled in the certification exams for advanced cybersecurity courses after only six months of coursework. Today, U.S. military and law enforcement agencies also rely on the CTE to find candidates for advanced training in cybersecurity, even among new recruits who had no prior idea that they could succeed in technical roles. The second evaluation tool is a gamified simulation platform in which each candidate takes on the role of Cyber Protection Agent and solves real-world cybersecurity challenges using tools and techniques that most candidates will have never before encountered. This simulation assessment has two impacts: it identifies curious, tenacious candidates who learn new techniques very fast (characteristics typical of elite cybersecurity practitioners), and second, it teaches candidates many of the underlying technologies that serve as underpinnings of cybersecurity, since the candidates realize that they have to use those technologies to solve the challenges. Affinity for and excellence in experiential learning is a robust identifier of people who will ultimately be elite cybersecurity practitioners.

## **2. Relation to the Mission and Strategic Goals of the SANS Technology Institute**

The mission of the SANS Technology Institute (STI) is to develop technically skilled professionals and leaders who strengthen global information security through innovative and flexible approaches to learning. The proposed Bachelor of Professional Studies in Applied Cybersecurity not only aligns with STI's mission but is core to accomplishing the mission and key strategic goals.

The first and most critical of STI's four strategic goals in its 2017–2021 Strategic Plan is to “materially increase the number of graduates prepared to lead and staff cybersecurity teams, programs, and efforts.” We have had success in producing graduates of the master's program who are making a profound difference in the cybersecurity posture of the organizations where they work, as documented in our Middle States' Self-Study Report prepared for the recently completed Team Visit Report to the Commission on Higher Education, and further recognized in the visiting team chair's report on that visit. However, STI is one of only a small number of institutions that is producing technical talent with deep hands-on mastery of cybersecurity, and all of those institutions together are producing only a tiny fraction of the people with advanced technical hands-on skills that the nation needs. STI is particularly limited in our student numbers because many excellent candidates have not completed an undergraduate degree and are thus not eligible for our master's degree. We believe this new program will increase the number of individuals entering the cybersecurity workforce with deep, hands-on mastery of cybersecurity and will also increase, over time, the number of students able to complete the STI master's degree program and go on to become cybersecurity leaders.

## **3. Funding for the Program**

STI's finances are sound. The school has adequate cash flow to fund the new program through to the time it breaks even, for five years if necessary. In addition, STI's parent organization, the SANS Institute, is willing and able to provide additional funds if needed.

#### **4. STI's Commitment to the Long-Term Success of the Program**

The BACS program will be critically valuable to STI in meeting its top strategic objective. Thus, the program has and will continue to have the highest visibility and priority for STI's president and administrative staff. Most BACS courses are central elements of the SANS Institute's catalog of professional development educational offerings, so students can count on those courses to be continually available and frequently updated for a sufficient time that students who enroll will be able to complete the program.

#### **B. Critical and Compelling Regional and Statewide Need as Identified in the State Plan**

##### **1a. Critical Need for the BACS Program**

Admiral Mike Rogers, then Commander of U.S. Cyber Command and Director of the National Security Agency (NSA), told the U.S. Congress in May 2017, "Every conflict around the world now has a cyber dimension. Cyber war is not some future concept or cinematic spectacle; it is real and here to stay." Admiral Rogers' successor, General Paul Nakasone, raised the priority of the cyber mission by establishing a new Cybersecurity Directorate with the mission "to prevent and eradicate threats." The level of hands-on skills needed to carry out that mission, both at NSA and at every company and agency that is a target of increasingly sophisticated attacks, is far higher than the level of talent currently available to them. They are competing with each other for the small number of people with elite hands-on skills, in a battle that the *Washington Post* has described as "fratricide," as discussed further in Section C.3 of this proposal

There has been widespread discussion of the need for high-performing professionals to help the United States prevail in cyber conflicts, a need not being met by current undergraduate cybersecurity programs. That need is pronounced both for military and intelligence organizations as well as for power, communications, and finance organizations and others that are part of the nation's critical infrastructure. What has not been so widely discussed is the extreme need for more cybersecurity professionals with hands-on advanced technical skills in specific roles in cybersecurity. Two seminal studies have documented the need for education such as that offered by STI's BACS program:

(1) A report by the Department of Homeland Security (DHS) Task Force on Cyber Skills, established by the DHS Secretary, concluded that to meet the nation's critical cyber manpower needs, the government should focus on education programs comprised of "courses with hands-on components and frequent testing that ensure actual mastery of the knowledge and skills." The report found that few colleges – even NSA-designated Centers of Academic Excellence – are graduating significant numbers of people with the hands-on technical skills needed by the nation. The report also isolated 10 "Red-Zone" jobs that the Task Force said were the most important mission-critical cybersecurity positions that the nation needs to fill. Each STI BACS graduate will have earned certifications indicating their readiness to take on Red Zone roles.<sup>1</sup>

<sup>1</sup> Department of Homeland Security, Task Force on Cyber Skills – Final Report.  
<https://www.dhs.gov/publication/homeland-security-advisory-council-cyberskills-task-force-report>, Accessed May 1, 2020



(2) A report by the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency concluded: “A critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where [the United States is] the weakest.” The bipartisan commission, which was chaired by a U.S. senator and a U.S. congressman, made two key recommendations: promote and fund the development of more rigorous curricula in our schools; and support the development and adoption of technically rigorous professional certifications that include a challenging educational and practical component.<sup>2</sup>

The demand from Maryland employers for people with the knowledge and hands-on skills that will be developed in the BACS program, and the demand from Maryland students for education that ensures they learn these hands-on skills, were both demonstrated when SANS (the parent of STI) announced the availability in January 2018 of 80 places in a non-credit program that includes two of the course and certification pairs of the BACS degree. Thirteen Maryland employers participated in the announcement and allowed SANS to include their logos and present their commitments in the program roll-out (see graphic with logos). These employers and a dozen others have hired more than 100 students who have now completed the non-credit program. Appendix 1 includes letters from two new Maryland employers expressing interest in hiring students with BACS degrees as well as letters from other employers expressing interest in hiring graduates who have earned the certifications that will be developed in the BACS program.



## 1b. The Key Benefit of BACS

Many employers have a requirement for a four-year degree to qualify for their cybersecurity jobs. BACS provides both the certified hands-on skills employers want and the bachelor's degree their human resources policies demand. Equally important, the response to the announcement of a non-credit program to earn two of the GIAC certifications in BACS showed that there is high student demand for such programs. To date, more than 2,300 Marylanders have applied for the ongoing non-credit program, which has a record of 91 percent placement in cybersecurity roles within nine months of program completion. We anticipate similar placement rates from BACS because BACS graduates will have mastered even more advanced security courses and certifications than the non-credit program.

BACS graduates will be able to excel in very challenging cybersecurity roles partly because of the STI courses they will complete and the five GIAC certifications they will earn. But their probability of success will be amplified further because, to be accepted into the BACS program, candidates will also have to excel in the two assessments that were described in the previous section: the psychometric CAT exam that assesses the way they approach problem-solving and compares their profile with profiles of people who are elite cybersecurity practitioners; and the

<sup>2</sup> Center for Strategic and International Studies, A Human Capital Crisis in Cybersecurity, Proficiency Matters. <https://www.csis.org/analysis/human-capital-crisis-cybersecurity>, Accessed May 1, 2020.

gamified simulation platform that gives candidates hundreds of cybersecurity challenges and allows them to demonstrate curiosity, tenacity, and the ability to learn new topics quickly – all core characteristics of elite cybersecurity practitioners. Success on those two assessments give students in the BACS program a head start in being selected for important cybersecurity roles and excelling in those roles.

Maryland has the highest concentration of any state of intelligence and military organizations with missions involving cybersecurity. World-class cyber skills are central to accomplishing those missions. Thus, it is appropriate that Maryland lead the nation in fostering education programs that produce graduates who impress those employers with the depth of their preparation and the value they can bring to the job from the first day.

Eliminating the gap between employer needs and college cybersecurity programs is a core national imperative (described by the DHS and CSIS studies cited above) that must be met if our nation hopes to protect our internet-dependent economy, our fully automated power and other critical infrastructure. The advanced courses and certifications students complete while earning their BACS degree offer proof the graduates have the skills needed to close that gap.

## **2. Alignment with the 2017–2021 Maryland State Plan for Postsecondary Education**

### ***New Partnerships between Colleges and Businesses***

The proposed program provides an innovative mechanism to implement Strategy 8 of the Maryland State Plan, which states: “Develop new partnerships between colleges and businesses to support workforce development and improve workforce readiness.” Specifically, BACS will prepare job-ready graduates to fill high-paying jobs offered by Maryland employers that have partnered with STI to help ensure the success of students. The corporations are not just being magnanimous. They need hands-on mastery of applied cybersecurity skills that they believe they can only get through programs that ensure that students pass rigorous certification exams prior to graduation. They pay for their existing employees to earn those certifications, so they are aware of the level of deep mastery and subsequent job success associated with those credentials. They are supporting STI in establishing an undergraduate curriculum that leads to those highly valued credentials because they feel they waste too much time and money providing additional critical training to employees who, in the employers’ view, should have come to them from colleges more job-ready. In sum, BACS provides a powerful example of a skills-development and industry certification-based undergraduate degree in Maryland.

### ***Increasing Student Success with Less Debt***

The BACS program will address the State Plan’s goals to increase student success with less debt. The cost of the program is far less than that of many four-year colleges because students will complete a portion of their coursework at community colleges. In addition, the Associate of Applied Science degree will be directly transferred into the BACS degree program, increasing the transferability of community college students into a bachelor’s degree program. When the BACS degree is added to the 60 to 70 hours students will have already completed at community colleges to earn their AA or AS degree, BACS students will save as much as 50 percent of the tuition they would have paid at four-year schools. Moreover, BACS graduates will have earned

at least five GIAC certifications, giving them a much greater chance of job placement success and higher salaries than graduates of other four-year programs who are often told they need to earn master's degrees, and take on even more debt, to learn the kind of advanced cybersecurity knowledge that will be taught to undergraduates at STI.

The BACS program also targets elements of two other Strategies in the Maryland State Plan. Strategy 7 calls for special efforts to support veterans. Since 2014, SANS has operated a support program for veterans. Our students who are veterans are having success in STI's challenging courses and certifications and are being hired at defense-oriented and other organizations that honor their sacrifice as well as their skill. Here's how U.S. Air Force Chief Master Sgt. Alexander Hall, 50th Network Operations Group Superintendent, described the STI program in an article published in 2014 by the Public Affairs Office of Schriever Air Force Base in Colorado, which supports Defensive Cyberspace Operations for the Air Force Space Command:

"We found Air Force IT personnel who were either separating or retiring, had certain levels of education or experience and who would be strong candidates. Finding approximately 600 people, we mailed them saying, 'We know you're leaving the Air Force soon, are you interested in giving this [program] a shot? [There's] no cost to you, and if you're successful, you're going to get a job.'

"The first pilot group to spearhead VetSuccess was assembled – nine Airmen in total. All passed with flying colors. The success of VetSuccess has only flourished to this day. During the last training cohort, every successful participant was negotiating for jobs making \$70,000 to \$120,000, just four months after leaving the service. To date, more than 80 veterans have been trained and taken valuable cybersecurity jobs.

"We know that IT veterans have all the things that the industry wants, what we're missing though, is the opportunity to put ourselves on display. That's what VetSuccess allows us to do; we go through industry standard training and certification to show ourselves off. Through this training we have proven that we know everything that our civilian counterparts know, and the IT industry is ready to hire us now."

And here's how one VetSuccess graduate described the program's impact on his life:

"Completing the SANS VetSuccess Academy not only influenced my career plans, it defined them. The education and certifications opened doors that were inaccessible to me otherwise, short of winning the lottery. In fact, being selected into the inaugural cohort was a 'hitting the jackpot' moment for me."

- Retired U.S. Air Force SMSgt Ed Russell, now employed at NTT Security

The BACS program would eliminate a major barrier and enable STI to do much more for veterans. Many veterans enroll in STI graduate certificate programs to master SANS material and make use of their VA education benefits. However, a substantial number of candidates are not eligible for admission to our graduate degree and certificate programs because they have not completed a four-year degree. The BACS program would provide a pathway for many previously ineligible veterans to take advantage of STI VA-eligible programs to earn STI cybersecurity degrees with widely-respected certifications, and to get the higher-paying jobs for which those certifications and four-year degrees qualify them.

Finally, Strategy 4 of the Maryland State Plan calls for collaboration between historically black universities and colleges (HBUCs) and other institutions to ensure equal educational opportunity for all Marylanders. SANS has optimized a cyber talent identification game that allows people who have never worked in IT to discover whether they would be good at cybersecurity and like it. We will make the same gamified simulation available to students in HBCUs that choose to be

partners, and we will follow up with additional support for the HBCUs to help their talented students pursue further study in cybersecurity and its foundations.

The effectiveness of the talent identification gamified simulation was demonstrated since 2018, during which time Maryland Governor Larry Hogan has partnered with SANS on the GirlsGoCyberStart Program. The results: approximately 300 Maryland high school girls signed up in 2018 and 500 in 2019. Maryland teams took four of the top six places among 2,700 teams from 17 states in 2018 and the top two spots in the nation in 2018. In 2020, the number of high school girls participating to date has increased to 597. The key takeaway from the program is that many young women who thought they would not be good at cybersecurity discovered their ability and are now interested in exploring a career in the field. The percentage of young women interested in a STEM/cybersecurity career grew from 35.6 percent before the girls used the simulator to 69.8 percent after they used it. The BACS program offers many of these students a cost-effective way to develop their talent and enter the cybersecurity field beginning at their local community colleges. We anticipate that the simulation game will discover talent in historically black institutions, as well as in community colleges, that may not have previously been recognized.

Towards an overall goal of increasing student success, SANS will make the talent identification simulator available to students in every one of the 16 Maryland community colleges that want to partner with SANS. This will open the door for talented students to discover their potential and to be seen as people who can make a difference in cybersecurity through the STI BACS program.

## **C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State**

### **1. Market Demand for Cybersecurity Professionals**

The National Institute of Standards and Technology (NIST) supports a website called CyberSeek that contains data on cybersecurity jobs and lists the number of current job openings by state and metropolitan area. In this section we combine the CyberSeek data with employment projections from the Maryland Department of Labor Licensing and Regulation (DLLR) to estimate the demand for the BACS program in Maryland and in the region.

CyberSeek states that the supply of cybersecurity workers nationally is “very low,” with 285,681 job openings relative to a total employed workforce of 746,858 (a ratio of 0.38, or, “for every 100 employed workers, the market seeks another 38 people”). The ratio of “openings requesting a GIAC certification” to “holders of GIAC certifications” is nearly twice as high at 0.64 (or, “for every 100 current GIAC certification holders, the market seeks another 64”). In Maryland alone, CyberSeek shows that there are 1,769 current job openings that specifically request GIAC certification holders. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job.

CyberSeek lists eight “top cybersecurity job titles” that are shown in Table 1, along with numbers of people in Maryland holding those jobs in 2014 and projected growth in demand for those jobs up to 2024. Clearly, not all these jobs can be called cybersecurity jobs. Yet, it is difficult to be hired into any of them without demonstrating a substantial knowledge of cybersecurity vulnerabilities and attack vectors that could disable the systems, networks, or software an employee will be developing or managing. Moreover, deep knowledge of hands-on cybersecurity like that gained in the BACS program can be a strong indicator of potential for rapid advancement and therefore a good reason to hire a candidate into any of these roles instead of other candidates who do not have the GIAC certifications earned by BACS students.

<b>Table 1. Current Positions and Projected Growth to 2024 in CyberSeek’s “Top Cybersecurity Job Titles”</b>			
<b>Job Title</b>	<b>Maryland Positions in 2014</b>	<b>Growth to 2024</b>	<b>Growth in Percent</b>
Cyber Security Engineer			
Cyber Security Analyst	3,514	1,829	52%
Network Engineer/Architect	5,678	1,534	27%
Cyber Security Manager/Administrator	9,780	2,494	25%
Software Developer/Engineer	29,677	10,423	35%
Systems Engineer			
Systems Administrator	14,206	3,606	25%
Vulnerability Analyst/Penetration Tester			
IT Auditor	28,974	6,282	22%
<b>Total</b>	<b>91,829</b>	<b>26,168</b>	<b>28%</b>

Source: <http://www.dllr.state.md.us/lmi/iandoproj/maryland.shtml> (accessed April 2, 2018).

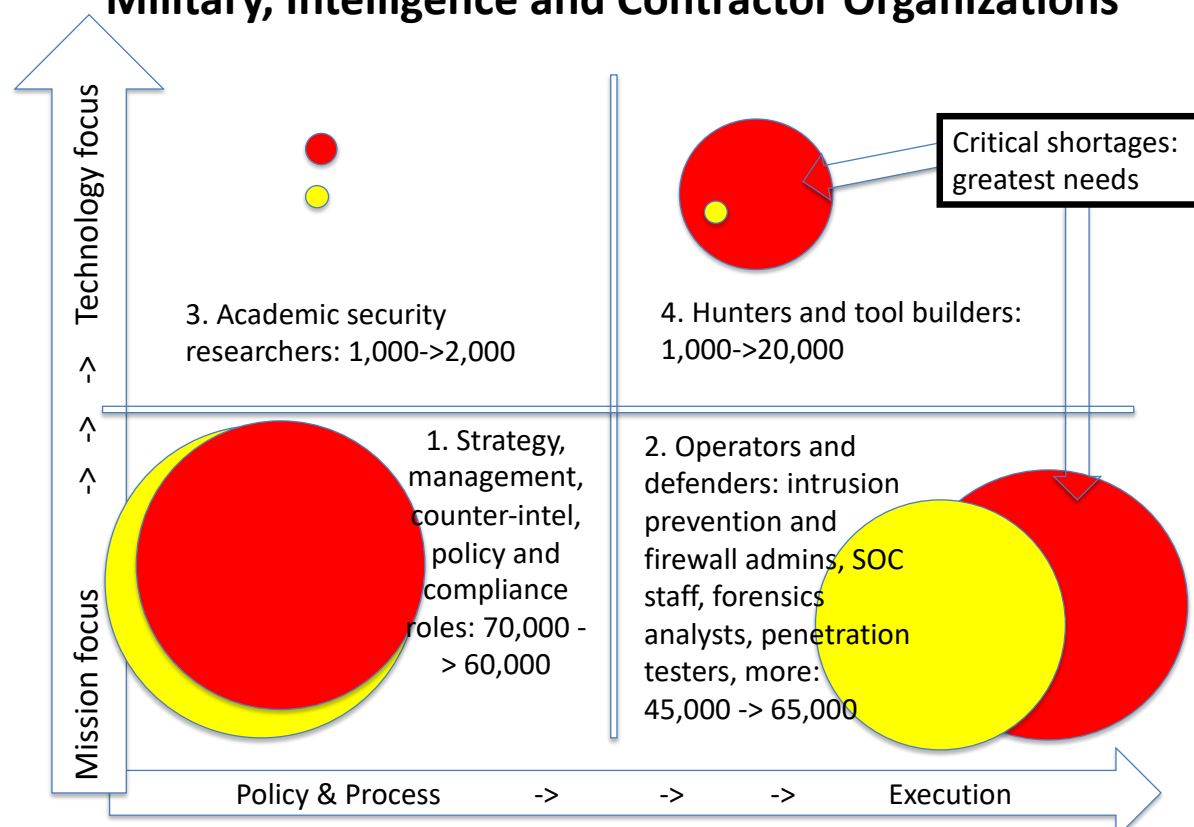
CyberSeek estimates the number of current cybersecurity job openings in Maryland at 14,535, which is not inconsistent with the DLLR numbers.

## 2. Demand for BACS Graduates

The BACS program is not targeting all of those openings, but rather the roles reserved for professionals with elite talent. BACS graduates will have a unique combination of high cyber aptitude, curiosity, tenacity, and rapid learning, along with hands-on expertise in important aspects of cybersecurity. In other words, they will be an elite cadre of cybersecurity graduates specifically educated to fill the most challenging of the red zone jobs identified by the Department of Homeland Security’s Task Force on CyberSkills. That begs the question, however, of how many elite cybersecurity practitioners employers actually need. That question was answered in a presentation at the last National Cybersecurity Symposium Executive Session conducted by the National Security Agency. At the session, the supply and demand chart below was shared with the flag-level military officers present at the Executive Session to help them understand why they were having such a hard time finding people to fill mission-critical (red zone) cybersecurity roles. The chart, designed in large part by the chief cryptographer of the

NSA, illuminates the extreme imbalance in the supply of and demand for cybersecurity professionals in the military/intelligence/aerospace segment of the U.S. economy, which employs a large share of the cybersecurity workforce in Maryland.

## Supply and Demand in Cyber Security Role Categories for Military, Intelligence and Contractor Organizations



This supply and demand chart shows estimates of the numbers of employees in cybersecurity roles in yellow and how many are needed in red. The quadrants range from largely policy and administrative roles in quadrant 1 to elite “hunters and tool builders” in quadrant 4. The professionals in quadrant 4 are expected to provide active defense, responding in near-real-time in the face of increasingly sophisticated nation-state attacks and capable of projecting power in cyberspace. Those professionals are not only needed on military teams but also to protect power, finance, communications, and other critical industries. When the next large war is waged, elite cybersecurity professionals will be as essential to victory as airplane pilots were in World War II.

What stands out in the chart is that the nation has a critical shortage, measured in tens of thousands, of elite technical professionals who can be the hunters and tool builders in quadrant 4 and the architects and technical leaders in quadrant 2. Those are the specific roles that BACS degree graduates will be destined to fill. BACS is not designed to prepare entry-level employees for quadrant 1 or the left side of quadrant 2. Those roles are being filled by graduates of existing cybersecurity degree programs.

In sum, we believe that nearly 60,000 elite cybersecurity workers are needed in the military/intelligence community/contractor workforce and the workforce of U.S. critical industries to enable the United States to withstand sustained cyber attacks in peacetime or when a war is being fought in cyberspace. A large fraction of those critical, unfilled jobs are in Maryland.

### 3. Current and Projected Supply of Cybersecurity Graduates

Two types of undergraduate programs seek to prepare people for cybersecurity roles: bachelor's degrees specifically in cybersecurity, and cybersecurity specializations within a bachelor of science computer science degree program. Table 2 shows data from the Maryland Higher Education Commission Secure Data Web Degree Trend website that summarizes degrees granted by all bachelor-level programs in cyber, computer, or information systems security in Maryland from 2012 to 2019.

<b>Table 2. Bachelor's Degree Programs in Cybersecurity in Maryland</b> <b>SOURCE:</b> <a href="https://data.mhec.state.md.us/mac_Trend.asp">https://data.mhec.state.md.us/mac_Trend.asp</a> Accessed April 15 2020			
School Name	Degree Level	Program Name	Degrees Granted, 2012–2019
Capitol Technology University	Bachelors	Cyber and Information Security	126
Frostburg State University	Bachelors	Secure Computing & Info Assurance	43
ITT Technical Institute	Bachelors	Information Systems Security	0
University of Maryland University College (UMUC)	Bachelors	Computer Networks & Security	4056
University of Maryland University College (UMUC)	Bachelors	Cybersecurity	2826

Another pathway for undergraduate students to prepare for jobs in cybersecurity is to enroll in a cybersecurity specialization within a computer science degree program. The Maryland Higher Education Commission Secure Data Web Degree Trend website shows 22 colleges offering computer science/computer engineering bachelor programs in Maryland. Table 3 lists those programs and shows, by shading, the six computer science bachelor's degree programs that offer, according to their computer science web page, a specialization in cybersecurity with a program of required courses or a concentration in cybersecurity without a required course of study.

**Table 3. Bachelor's Degree Programs in Computer Science/Computer Engineering in Maryland with and without Specializations in Cybersecurity**

School Name	Degree Level	Program Name	Degrees Granted, 2012–2019	Specialization in Cybersecurity
University of Maryland, College Park	Bachelors	Computer Science	3249	Yes
University of Maryland, Baltimore County	Bachelors	Computer Science	1503	Concentration
University of Maryland Global College	Bachelors	Computer Science	1358	No
Towson University	Bachelors	Computer Science	659	Yes
Johns Hopkins University	Bachelors	Computer Science	475	Yes
Stevenson University	Bachelors	Computer Information Systems	378	Yes - forensics
Bowie State University	Bachelors	Computer Science/Computer Technology	329	Yes
Frostburg State University	Bachelors	Computer Science/Information Systems	198	No
Salisbury University	Bachelors	Computer Science	197	No
St. Mary's College of Maryland	Bachelors	Computer Science	145	No
Capitol Technology University	Bachelors	Computer Science/Computer Engineering	128	No
University of Maryland, Eastern Shore	Bachelors	Computer Science Data Processing	106	No
Morgan State University	Bachelors	Computer Science	95	No
Hood College	Bachelors	Computer Science	92	No
Loyola University Maryland	Bachelors	Computer Science	80	No
McDaniel College	Bachelors	Computer Science	59	No
Mount St. Mary's University	Bachelors	Computer Science	58	No
Coppin State University	Bachelors	Computer Science	45	No
Washington College	Bachelors	Computer Science	44	No
Goucher College	Bachelors	Computer Science	37	No
Washington Adventist University	Bachelors	Computer Science	15	No
Notre Dame of Maryland University	Bachelors	Computer Information Systems	12	No



No data have been published on the number of students earning computer science degrees with specializations in cybersecurity. Our belief is that the number of job openings for employees with substantial hands-on mastery of advanced topics in cybersecurity – as demonstrated by their passing rigorous, nationally standardized certification exams – is substantially greater than the number of graduates with those skills being produced by the two types of programs listed in this section. That conclusion is supported by the employers’ letters of support and student demand for places in the SANS nondegree program. As noted above, there is substantial demand from employers and students alike for a program like the BACS, where students, as part of their degree, prove their mastery of advanced topics in cybersecurity by passing widely used advanced certification exams.

In sum, thousands of students are graduating from Maryland colleges each year with degrees in cybersecurity and computer science with a cybersecurity specialization. A few of those students develop elite hands-on capabilities through extracurricular activities in cybersecurity competition clubs and by building home networks as hobbyists. That small number, however, is insufficient to meet the needs for elite talent even for just the NSA. Here’s how Ellen Nakashima describes the competition for elite cyber talent in an article in the *Washington Post*: “Along the Baltimore-Washington Parkway, the concentration of government agencies and contractors brimming with computer geeks rivals any cyber defense area on the planet. And in this age of growing cyber threats, those firms are engaged in a cyber-hiring competition so fierce that one expert called it “fratricide on the parkway.” Nakashima quotes a cybersecurity hiring manager: “We are all hiring away from each other. I’m doing it myself. They’re all going to the highest bidder.” In other words, elite cybersecurity practitioners are in short supply.

#### **D. Reasonableness of Program Duplication**

##### **1. Similarities and Differences between the BACS Program and Other Programs Awarding Bachelor’s Degrees in Cybersecurity**

*In determining whether a program is unreasonably duplicative, according to the Maryland Code of Regulations (COMAR 13B.02.03.09(C), the Secretary shall consider (a) the degree to be awarded; (b) the area of specialization; (c) the purpose or objectives of the program to be offered; (d) the specific academic content of the program; (e) evidence of equivalent competencies of the proposed program in comparison to existing programs; and (f) an analysis of the market demand for the program. The analysis on unreasonable duplication shall include an examination of factors including (a) the role and mission; (b) accessibility; (c) alternative means of educational delivery, including distance education; (d) analysis of enrollment characteristics; (e) residency requirements; (f) admissions requirements; and (g) educational justification for the dual operation of programs broadly similar to unique or high-demand programs at historically black institutions.*

Our analysis of these factors demonstrates that the STI BACS program is not unreasonably duplicative, and that it is an important addition to the educational offerings available to students in Maryland.

##### ***Specific Academic Content of the Program; Evidence of Equivalent Competencies***

The BACS program offers students program elements not currently available in any other accredited bachelor's degree program:

1. *Five GIAC certifications.* Other colleges in Maryland offer courses designed to prepare students to take cybersecurity certifications, but no other BS program requires graduates to have actually passed advanced cybersecurity certifications as a graduation requirement. Further, none of those programs include passing GIAC certification exams, which require the student to demonstrate hands-on mastery of the skills being evaluated. GIAC certifications are used by the U.S. Department of Defense to qualify employees for advanced cybersecurity roles.
2. *Effective security writing and speaking.* Many programs include requirements for business writing. BACS goes further, teaching students how to write the most common security reports, including after-action incident reports, threat reports, malware reports, and several others. It covers elements that should be included in such reports, how to present them, how to illustrate them for maximum impact, and, an area of particular concern in cybersecurity writing, what to leave out. BACS also teaches students how to present cybersecurity information or maximum impact with specific guidance on threat briefings, incident reports, security awareness briefings, and briefings to executives and boards of directors.
3. *An internship with organizations operating national and global cybersecurity monitoring programs.*

### ***Alternative Means of Educational Delivery, including Distance Education***

The BACS program will, when the current pandemic subsides, require students to attend some of their advanced cybersecurity courses in person in classrooms where they can master the hands-on skills needed to accelerate their careers. The face-to-face classes are usually accompanied by evening NetWars competitions where students can hone their skills in competition with other students. In contrast, most current cybersecurity bachelor's degree students at Maryland colleges are attending programs that are 100 percent online.

### ***Role and Mission***

BACS specifically targets preparing the hunters, tool builders, tech directors, and architects who are critically needed by military and commercial organizations. BACS is not competing with other Maryland cybersecurity programs that are preparing most graduates for security compliance roles or information security analyst roles, or to become security-savvy system and network administrators and help-desk professionals.

## **2. Admissions Requirements**

STI's admission requirements for the BACS require a 3.0 GPA, in contrast with the largest current Maryland cybersecurity programs that require a 2.0 GPA. This difference allows STI to accelerate the learning process and expect a much higher level of performance from our students. Even more importantly, the BACS admission process includes both a psychometric test of cybersecurity aptitude and a gamified simulator that allows candidates to demonstrate they have what it takes become formidable cybersecurity professionals. The simulator is remarkably effective in identifying people with talent for excellence in cybersecurity, even those who had no prior idea that they had that talent. The United Kingdom adopted the same simulator as the core

of its \$25 million HMG CyberDiscovery Programme launched in November 2017 to identify candidates to be developed into elite cybersecurity analysts for the UK military and intelligence community as well as other employers. The success of that program in identifying thousands of people who have demonstrated remarkable cybersecurity talent adds to our confidence that BACS graduates will excel in this difficult and important field.

By accepting students who have demonstrated outstanding talent through the aptitude test and gamified simulator, STI can accelerate the student learning process by enabling a focus on rich academic content and advanced competencies.

**E. Relevance to High-Demand Programs at Historically Black Institutions (HBIs)**

Not applicable

**F. Relevance to the Identity of Historically Black Institutions (HBIs)**

Not applicable

**G. Adequacy of Curriculum Design and Delivery to Related Learning Outcomes (COMAR 13B.02.03.10)**

**1. Describe how the proposed program was established, and also describe the faculty who will oversee the program.**

BACS was established as a means of meeting STI's strategic goal of "materially increasing the number of graduates prepared to lead and staff cybersecurity teams, programs, and efforts." Our faculty and administrators recognized that students who have completed two years of college who can demonstrate high aptitude for careers in cybersecurity constitute a large group of potential professionals who could, if provided accelerated cybersecurity education, quickly become elite members of cybersecurity teams. From the outset the program has been designed in cooperation with a team from Montgomery College to ensure that it can be implemented without putting undue stress on community colleges. In addition, as described in Section H below, SANS consulted with Maryland community college presidents and chief academic officers in designing the program in order to make the transition from community college to the Bachelor of Professional Studies in Applied Cybersecurity as smooth and stress-free as possible for both students and community colleges.

An STI Bachelor of Professional Studies in Applied Cybersecurity will provide an opportunity for those high-potential students to complete a very challenging program that includes advanced immersion training in cybersecurity practice, as well as earn certifications that affirm their mastery of those advanced topics. In this way, the BACS will enable students capable of becoming elite cybersecurity practitioners to earn an undergraduate degree that makes them demonstrably desirable for high-impact cybersecurity jobs and immediately employable upon graduation. The BACS is a natural extension of STI's current upper

division Applied Cybersecurity Certificate that offers many of the same benefits. But the BACS adds the benefits of enabling STI students to (1) complete more GIAC certifications (2) complete their undergraduate degree at STI and (3) earn a prestigious SANS Technology Institute bachelor's degree.

The faculty that will serve the students of the proposed BACS program is made up of the same widely respected scholar-practitioners who currently teach the 800 enrolled graduate students at the SANS Technology Institute and the 200 students enrolled in the current upper division ACS certificate program. A detailed list of the STI faculty and their credentials, along with biographical sketches of selected leading faculty members, are provided in Section I below.

## **2. Describe educational objectives and learning outcomes appropriate to the rigor, breadth, and (modality) of the program.**

a) The BACS program is designed to provide an accelerated path for holders of AAS degrees who can demonstrate a high level of aptitude for cybersecurity-related work to enter the workforce and quickly meet the needs of employers. They will stand out from other bachelor's degree holders because they will enter the workforce with a credible and applicable set of skills that are attractive to employers. Graduates will attain jobs with above-average compensation and promising career prospects because they will have demonstrated the hands-on skills to immediately take on the following important responsibilities:

- Assess an organization's information systems to identify exploitable cybersecurity vulnerabilities and perform needed mitigation tasks to eliminate or mitigate those vulnerabilities
- Evaluate the cyber hygiene of an organization using the Critical Security Controls and the NIST Framework
- Conduct incident analysis to identify elements of the kill chain that may have failed and thus allowed intruders to gain a foothold in the organization's computers and networks
- Write substantive management reports on cyber hygiene, security tools, malware, and threats, as well as after-action incident reports
- Provide management briefings on security tools, malware, threats, and incident analyses
- Assess a proposed new software and hardware system to find probable security flaws
- Demonstrate specialized mastery in an advanced area of cybersecurity. ranging from industrial control systems to forensics and web application penetration testing.

To meet those objectives the STI BACS program will enable students to achieve the following learning outcomes:

- Demonstrate hands-on familiarity with the foundational technologies upon which cybersecurity excellence is built, including computer architecture, networking, programming and scripting, and Linux and Windows operating systems

- Assess cyber hygiene using the seven key Critical Security Controls and show how those specific controls enable the elements of the NIST Cybersecurity Framework
- Solve dozens of real-world cybersecurity problems in a simulated but realistic computing environment
- Assemble tools and configure systems and networks to permit them to foster resiliency and continuity of operations through attacks
- Demonstrate competence in the use of common security tools to secure Windows and Linux systems, assess vulnerabilities and exploits, and excel in the advanced area of specialization they choose.
- Demonstrate mastery of each of the learning objectives required for the advanced BACS cybersecurity courses such as those listed below.
- Write security reports and present security briefings competently
- Complete Maryland state-mandated General Education requirements

In addition, each advanced security course in the STI BACS program has 10-30 specific learning objectives. Lists of learning objectives are referenced in Section 3 below. They show how student mastery of the learning objectives is assessed. Below, as an example, is the list of learning objectives for ACS 3504: GIAC Security Incident Handling and Hacker Exploits, which is assessed in the GCIH (GIAC Certified incident Handler) Certification Exam.

- Incident Handling: Identification  
The candidate will demonstrate an understanding of important strategies to gather events, analyze them, and determine if we have an incident.
- Incident Handling: Overview and Preparation  
The candidate will demonstrate an understanding of what Incident Handling is, why it is important, and the best practices to take to prepare for an incident.
- Client Attacks  
The candidate will demonstrate an understanding of various client attacks and how to defend against them.
- Covering Tracks: Networks  
The candidate will demonstrate an understanding of how attackers use tunneling and covert channels to cover their tracks on a network, and the strategies used to defend against them.
- Covering Tracks: Systems  
The candidate will demonstrate an understanding of how attackers hide files and directories on Windows and Linux hosts and how they attempt to cover their tracks.
- Denial of Service Attacks  
The candidate will demonstrate a comprehensive understanding of the different kinds of Denial of Service attacks and how to defend against them.
- Incident Handling: Containment  
The candidate will demonstrate an understanding of high-level strategies to prevent an attacker from causing further damage to the victim after discovering the incident.

- Incident Handling: Eradication, Recovery, and Lessons Learned  
The candidate will demonstrate an understanding of the general approaches to get rid of the attacker's artifacts on compromised machines, the general strategy to safely restore operations, and the importance of the incident report and lessons learned meetings.
- Network Attacks  
The candidate will demonstrate an understanding of various network attacks and how to defend against them.
- Overflow Attacks  
The candidate will demonstrate an understanding of how overflow attacks work and how to defend against them.
- Password Attacks  
The candidate will demonstrate a detailed understanding of the three methods of password cracking.
- Reconnaissance  
The candidate will demonstrate an understanding of public and open-source reconnaissance techniques.
- Scanning: Discovery and Mapping  
The candidate will demonstrate an understanding of scanning fundamentals in order to discover and map networks and hosts, and reveal services and vulnerabilities.
- Scanning: Techniques and Defense  
The candidate will demonstrate an understanding of the techniques and tools used in scanning, and how to prepare against scanning and respond to it.
- Session Hijacking and Cache Poisoning  
The candidate will demonstrate an understanding of tools and techniques used to perform session hijacking and cache poisoning, and how to prepare for and respond to these attacks.
- Techniques for maintaining access  
The candidate will demonstrate an understanding of backdoors, trojan horses, and rootkits operate, what their capabilities are, and how to defend against them.
- Web Application Attacks  
The candidate will demonstrate an understanding of the value of the Open Web Application Security Project (OWASP), as well as different Web App attacks such as account harvesting, SQL injection, Cross-Site Scripting, and other Web Session attacks.
- Worms, Bots, and Bot-Nets  
The candidate will demonstrate a detailed understanding of what worms, bots, and bot-nets are and how to protect against them.

- 3. Explain how the institution will:**
- a) provide for assessment of student achievement of learning outcomes in the program**
  - b) document student achievement of learning outcomes in the program**

STI measures student achievement of learning outcomes in the advanced security courses using the Global Information Assurance Certification (GIAC) examination associated with each of the advanced security courses that the student completes. These certification examinations are globally standardized, and they measure more than just the ability to answer multiple-choice questions. In several certifications, including GCIH, the certification exam for ACS504, students must demonstrate the ability to apply what they learned in solving problems in actual computer environments, GIAC certification exams are used by tens of thousands of security professionals each year. For example, the two core certification exams (GSEC and GCIH) have been attempted by more than 53,000 professionals, and nearly 45,000 have succeeded in earning those certifications.

The latest versions of the learning objectives for a representative subset of the BACS courses, measured by the relevant GIAC exams, may be found at the following links for the respective certifications:

- For ACS 3401: GIAC Security Essentials Certification Exam (GSEC)  
<https://www.giac.org/certification/security-essentials-gsec>
- For ACS 3504: GIAC Security Incident Handling and Hacker Exploits Certification Exam (GCIH)  
<https://www.giac.org/certification/certified-incident-handler-gcih>
- For ACS 4503: GIAC Certified Intrusion Analyst (GCIA)  
<https://www.giac.org/certification/certified-forensic-examiner-gcfe>
- For ACS 4410: Certified Industrial Cybersecurity Professional Exam (GICSP)  
<https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp>
- For ACS 4501: Certified Enterprise Defender Exam (GCED)  
<https://www.giac.org/certification/certified-enterprise-defender-gced>
- For ACS 4503: Certified Intrusion Analyst Exam (GCIA)  
<https://www.giac.org/certification/certified-intrusion-analyst-gcia>
- For ACS 4542: Certified Web Application Penetration Tester Exam (GWAPT)  
<https://www.giac.org/certification/certified-web-application-penetration-tester-gwapt>

<https://www.giac.org/certification/web-application-penetration-tester-GWAPT>

- For ACS 4560: Certified Penetration Tester Exam (GPEN)  
<https://www.giac.org/certification/penetration-tester-gpen>

Certification exams that will be used by the BACS program are in turn certified by the American National Standards Institute. Learning objectives are updated at least every three years after the assessment of rigorous, detailed, and updated job task analyses that have made the passing of these exams globally recognized as being indicative of having mastered the knowledge taught in our technical courses and the capabilities required to engage in real-world cybersecurity activities. Because no students will be awarded a BACS degree if they fail to pass any of the GIAC exams required by the program, student success on the GIAC exams correlates to achievement of the learning outcomes targeted by the BACS program.

Achievement of the learning objectives for the foundational technologies are measured primarily through examinations prepared by the faculty teaching each base technology. The students' mastery of the foundations will be reinforced and validated in STI's upper division courses and the GIAC certification examinations.

STI employs a second assessment program to ensure the school is continuously delivering its courses with a high degree of professionalism as seen from the student perspective. In every course, every day, every student is asked to complete an assessment of the instructor, the labs, the content, the delivery platform, and more. Approximately 60% of all students comply. These assessments are processed overnight. On rare occasions when a teacher appears to be failing, whether for health reasons or otherwise, a backup teacher is brought in the next day to help or replace the current teacher. Such interventions are rarely needed, but their availability and (infrequent) application help make learning at STI a consistent and remarkably positive and effective experience for the students.

#### **4. Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements**

To earn the BACS degree a student will have completed 120 credit hours of coursework of which at least 40 credit hours will be general education. In addition, the student will complete 45 credit hours in the major of which 24 are in upper division courses. The table below summarizes the coursework that a BACS student will complete in meeting the requirements for a Bachelor of Professional Studies in Applied Cybersecurity. The courses with shaded background will be completed prior to entering the Bachelor of Professional Studies BACS program and will be transferred to STI under articulation agreements with Montgomery College, other Maryland community colleges and other colleges. Courses with a (U) in the credit hours column are upper division courses.



<b>Table 1: BACS Program Articulation Roadmap with Montgomery College</b>			
<b>BACS Degree General Education Requirements</b>	<b>MC Course (credit hours)</b>	<b>STI Course (credit hours)</b>	<b>General Education or Major</b>
Arts and Humanities	(3)		General Education
College Writing	ENGL101 (3)		General Education
Introduction to Ethics	PHIL 140 (3)		General Education
Mathematics	(3)		General Education
Natural science with lab	(4)		General Education
Interpersonal Communications	COMM 108 (3)		General Education
Business and Professional Communications	COMM 112 (3)		General Education
Research and Writing in the Workplace	ENGL 103 (3)		General Education
Effective Cyber Writing and Speaking		ACS 4023 (3)	General Education
Four General Education Electives	(12)		General Education
Microcomputer Essentials	NWIT 127 (3)		Major
Introduction to Networking	NWIT 151 (3)		Major
Microsoft Windows Server	NWIT 203 (3)		Major
Cisco Networking 2	NWIT 252 (3)		Major
UNIX/LINUX System Administration	CMSC 253 (3)		Major
Six Courses Required for the AAS Degree and Electives	(18)		Major or other
Technology Essentials		ACS 3201 (6)	Major
Introduction to Cybersecurity		ACS 3301 (4)	Major
Security Essentials		ACS 3401 (6)	Major
Automating Information Security with Python		ACS 3573 (4)	Major
Intrusion Detection In-Depth		ACS 3503 (6)	Major
Incident Handling and Hacker Exploits		ACS 3504 (6)	Major
Three Upper-Division Cybersecurity Specialization Electives		(9)	Major
Internship		ACS 3499 (6)	Major
<b>TOTAL BY INSTITUTION</b>	<b>70</b>	<b>50</b>	
<b>TOTAL FOR BACS DEGREE</b>	<b>120</b>		

### **BACS:**

*Cybersecurity Specialization Electives:* Each student must complete three of these upper division specialization courses. Students who have previously taken courses equivalent to BACS required courses may either take additional advanced electives from this list or take additional foundational courses, or a combination of these two options, in order to better prepare them for the advanced cybersecurity courses. The decision on which courses to take as replacements for previously completed courses will be made by the student in consultation with his/her STI counselor. All cybersecurity specialization electives earn 3 credit hours. The standardized certification exam, which must be passed to earn credit for the course, and which leads to

certification in each advanced cybersecurity skill area, is listed in parentheses following the course name.

Upper Division Electives:

- ACS 3504: Intrusion Detection In-Depth (GCIA)
- ACS 3505: Securing Windows and PowerShell Automation (GCWN)
- ACS 3502: Securing Linux/Unix (GCUX)
- ACS 3511: Continuous Monitoring and Security Operations (GMON)
- ACS 3522: Defending Web Applications Security Essentials (GWEB)
- ACS 3530: Defensible Security Architecture and Engineering (GDSA)
- ACS 3540: Cloud Security and DevOps Automation (GCSA)
- ACS 3542: Web App Penetration Testing and Ethical Hacking (GWAPT)
- ACS 3555: SIEM with Tactical Analytics (GCDA)
- ACS 3560: Network Penetration Testing and Ethical Hacking (GPEN)
- ACS 3566: Implementing and Auditing the Critical Security Controls – In-Depth (GCCC)
- ACS 3575: Mobile Device Security and Ethical Hacking (GMOB)
- ACS 3599: Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses (GDAT)
- ACS 4642: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (GXPN)
- ACS 3500: Windows Forensic Analysis (GCFE)
- ACS 3508: Advanced Incident Response, Threat Hunting, and Digital Forensics (GCFA)
- ACS 3572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (GNFA)
- ACS 3578: Cyber Threat Intelligence (GCTI)
- ACS 3585: Smartphone Forensic Analysis In-Depth (GASF)
- ACS 3560: Reverse-Engineering Malware: Malware Analysis Tools and Techniques (GREM)
- ACS 3507: Auditing & Monitoring Networks, Perimeters & Systems (GSNA)
- ACS 3410: ICS/SCADA Security Essentials (GICS)
- ACS 3523: Law of Data Security and Investigations (GLEG)
- ACS 3414: SANS Training Program for CISSP® Certification (GISP)
- ACS 3512: Security Leadership Essentials for Managers (GSLC)
- ACS 3514: Security Strategic Planning, Policy, and Leadership (GSTRT)
- ACS 3525: IT Project Management, Effective Communication, and PMP® Exam Prep (GCPM)

The course content and learning objectives are described in detail below in alpha order by course designation. Where GIAC certification exams are applicable they are listed at the end of each list of learning objectives:

**ACS 3201: Technology Essentials**

ACS 3201 is an extensive and intensive hands-on course designed to ensure each BACS student has baseline mastery of the fundamental technologies that underpin and define cybersecurity, and that serve as a preparatory step for ACS 3401. Regardless of their individual starting points,

students will develop required knowledge of topics ranging from the architecture of modern computers to topics that cover how a CPU works, at a level that enables students to understand how malicious actors can suborn CPU processes, including the addressing of memory and the relationships between hardware and operating systems. It similarly covers networking and network protocols, Linux, Python programming, and other foundational topics. The goal is not for students to be experts in these technologies, but rather for them to be able to understand and have hands-on engagement with them to a degree sufficient for the practice of information security. That level of mastery has proven entirely sufficient for most students to excel in challenging immersion courses that characterize STI advanced cybersecurity courses.

Through an online platform, students in this course engage in more than 40 hours of “seat time” augmented with labs, quizzes, Q&A with instructors, and ample outside work that reinforces the concepts taught. Instructional modules are stacked so that concepts are progressively built up and a detailed understanding is developed. Students study a diverse set of topics that slowly increase in difficulty until they grasp each concept, rather than being overloaded with information on a single topic. Students with little background are able to move at a slower pace in earlier modules and levels of the simulation, while students who have some related understanding will complete earlier modules quickly and move on to topics they don’t already know.

The online platform also features web-based access to virtualized labs, enabling students to get hands-on practice with Linux commands and solve security problems without the difficulty of setting up infrastructure. This significantly reduces the barrier to entry and allows for transition from theory to hands-on exercises for a more engaging student experience.

ACS 3201 also teaches logic, programming, and scripting and introduces how each of these can lead to errors that allow security experts or cyber criminals to find faults and exploit them.

*Assessments:* 46 quizzes and exams throughout the course plus an examination covering the full course.

### **ACS 3301: Introduction to Cyber Security**

Upon completion of this course a student will be able to demonstrate an understanding of:

- Access controls and effective authentication, authorization, and accountability
- Securing applications from malware and other common threats
- Foundational numbering systems
- Cryptographic algorithms
- Cryptography and its application
- Cryptography throughout history
- Network addressing and protocols
- Network attacks, at a foundational level
- Network concepts and terminology
- Countermeasures and technologies employed to minimize the associated risks from attacks
- Fundamental information security and risk management concepts as well as the components of effective policy creation and awareness programs

- Securing systems from common threats
- Wireless technologies as well as the defenses employed to minimize the associated risks from wireless attacks

*Assessment:* GIAC Information Security Foundations certification exam

### **ACS 3401: Security Essentials**

ACS 3401 is the introductory, technically oriented BACS course on information security. It establishes the foundations to design, build, maintain, and assess security functions at the end-user, network, and enterprise levels of an organization. This course will prepare students to design and build a network architecture using VLANs, NAC, and 802.1x based on an APT indicator of compromise; run Windows command line tools to analyze the system looking for high-risk items; run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools; install VMWare and create virtual machines to operate a virtual lab to test and evaluate the tools/security of systems; create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness; and identify visible weaknesses of a system using various tools, including dumpsec and OpenVAS, and once vulnerabilities are discovered cover ways to configure the system to be more secure. ACS 3401 is an extended version of SANS course SEC401, tailored to the CACS BACS and adding significant time and exercises to master the underlying foundations on which successful technical cybersecurity careers are built.

*Assessment:* GIAC Security Essentials Certification (GSEC) examination

### **ACS 3503: Intrusion Detection In-Depth**

ACS 3503 may be the most important course that elite cybersecurity professionals take because it enables them to be ready to respond to emerging threats. It develops the skills to deeply understand what is happening on a network today, and to find the very serious things happening right now that none of the commercial tools are telling them about. In this way it is very different from most college courses covering intrusion detection that focus on using commercial tools. ACS 3503 teaches you how and why TCP/IP protocols work the way they do, common application protocols and a general approach to researching and understanding new protocols. The result is that students will leave this class with a clear understanding of how to instrument their network and the ability to perform detailed incident analysis and reconstruction. Coverage beyond a deep expertise in TCP/IP include (1) crucial application protocols: DNS, HTTP(S), SMTP, and Microsoft communications, (2) protocol analysis, a key skill in intrusion detection, (3) IDS/IPS evasion techniques, the bane of the analyst, practical and advanced techniques in using SNORT and ZEEK, network forensics analysis, using network flow records, examining command and control traffic, analysis of large pcaps, and ends with a challenging but fun, hands-on, score-server-based IDS challenge in which students compete to answer many questions that can only be answered if they can actually use the tools and techniques covered in the course.

*Assessment:* GIAC Certified Intrusion Analyst (GCIA) examination

These benefits alone make this training completely worthwhile. What makes the course as important as we believe it is (and students tell us it is), is that we force you to develop your critical thinking skills and apply them to these deep fundamentals. This results in a much deeper understanding of practically every security technology used today.

### **ACS 3504: Incident Handling and Hacker Exploits**

By adopting the viewpoint of a hacker, ACS 3504 provides an in-depth look into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling. Students will learn to apply incident handling processes – including preparation, identification, containment, eradication, and recovery – in order to protect enterprise environments; analyze the structure of common attack techniques to evaluate an attacker's spread through a system and network in order to anticipate and thwart further attacker activity; use tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and Trojan horses, choosing appropriate defenses and response tactics for each; use built-in command-line tools such as Windows tasklist, wmic, and reg, as well as Linux netstat, ps, and lsof, to detect an attacker's presence on a machine; analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect; use memory dumps and memory analysis tools to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network; gain access to a target machine using Metasploit, and then detect the artifacts and impact of exploitation through process, file, memory, and log analysis; analyze a system to see how attackers use the malware to move files, create backdoors, and build relays through a target environment; run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impact of the scanning activity; apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics; employ the netstat and lsof tools to diagnose specific types of traffic-flooding denial-of-service techniques, and choose appropriate response actions based on each attacker's flood technique; and analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors. This course is an extended version of SANS course SEC504, adding extensive study of actual attacks and a student project to develop a profile of a major attack, present it to the community through a YouTube video, and evaluate other students' attack profile presentations.

*Assessment:* GIAC Certified Incident Handler (GCIH) examination

### **ACS 3573: Automating Information Security with Python**

ACS 3573 provides the skills cybersecurity professionals need for tweaking, customizing, or outright developing their own tools. It puts them on the path to creating their own tools, empowering them to better automate the daily routine of today's information security professional and to achieve more value in less time. Again and again, organizations serious about

security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it.

Upon completion of this course, a student will be able to:

- Leverage Python to perform routine tasks quickly and efficiently
- Automate log analysis and packet analysis with file operations, regular expressions, and analysis modules to find evil
- Develop forensics tools to carve binary data and extract new artifacts
- Read data from databases and the Windows Registry
- Interact with websites to collect intelligence
- Develop UDP and TCP client and server applications
- Automate system processes and process their output

*Assessment:* GIAC Python Coder (GPYC) examination

### **ACS 4023: Effective Cybersecurity Writing and Presentations**

Upon completion of this course, a student will be able to:

(Writing segment)

- Describe the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing
- Make these elements part of their arsenal through hands-on exercises that draw on common security scenarios
- Learn the key topics needed to address in security reports and other written communications, with a focus on commonly required reports including:
  - Cybersecurity Incident Reports
  - Pen Testing and Other Security Assessment Reports
  - Malware and Other Threat Reports
- Understand how to pick the best words, structure, look, and tone
- Begin improving skills at once by spotting and fixing weaknesses in security samples
- Take advantage of practical checklists provided in the course to ensure writing is clear and effective
- (Presentation segment)
- Gain and hold security audiences' attention:
  - Project authority, energy, and awareness
  - Develop effective non-verbal communication skills
  - Identify common presentation mistakes
  - Develop strategies to reduce anxiety when speaking
  - Effectively manage interruptions
- Package information for maximum acceptance by technical and management audiences
  - Set up the presentation to gain audience trust
  - Identify common errors when opening
  - Solve voice challenges
  - Use visuals effectively

- Develop and use techniques to respond to all types of questions
- Employ lessons from real-world security presentation successes and catastrophes
  - How and when to use stories
  - How to create an effective outline
  - How to use timelines effectively
  - How examples can reinforce your position
  - How to persuade management to take action
  - How to effectively use reference metrics
- Learn formats (and what to avoid) for specific cybersecurity presentations
  - Presenting a security awareness briefing
  - Presenting a new tool
  - Presenting an incident report
  - Presenting cybersecurity status to management and boards of directors
  - Use presentation speaker rating forms to continuously improve your presentations.

### **CMSC 253: UNIX/Linux System Administration**

Upon completion of this course, a student will be able to:

- Install a UNIX/LINUX operating system
- Configure a UNIX/LINUX kernel
- Describe a UNIX/LINUX system architecture
- Describe the administrative tasks of the OS
- Utilize system utilities to perform administrative tasks
- Run and configure essential system processes
- Describe the file system hierarchy
- Create and maintain file systems
- Perform backup and recovery
- Create and maintain users and groups
- Install and configure application software
- Manage and configure devices
- Install and configure network components

### **COMM 108: Interpersonal Communications**

Upon completion of this course, a student will be able to:

- Identify effective communication skills to help reduce anxiety and apprehension in dealing with others
- Describe guidelines for self-disclosure in intimate relationships
- Define major types of conflict, contexts that contribute to conflict, and appropriate conflict management styles
- Identify communication guidelines for establishing successful relationships using computer-mediated communication
- Apply interpersonal communication skills that are appropriate for professional relationships

- Describe and apply active and critical listening skills
- Differentiate between describing and displaying feelings in relationships
- Identify appropriate personal communication behaviors that contribute to effective communication with others

### **COMM 112: Business and Professional Communications**

Upon completion of this course, a student will be able to:

- Differentiate between the various types of communication (one-on-one, small group, and public) and develop effective strategies for each
- Explain the human communication process within an organization
- Identify appropriate channels and networks for effective communication within an organization
- Explain how communication lines can break down and develop strategies to prevent such breakdowns
- Assess different communication styles among gender and ethnic groups and other culturally diverse populations within an organization itself
- Identify and critically evaluate the two main types of messages within an organization: the informative and persuasive
- Explain how presentations fit into the corporate structure, and subsequently organize and deliver such presentations
- Demonstrate effective communication skills in order to solve problems as part of a team
- Integrate technology including PowerPoint presentations in informative and persuasive speeches
- Design appropriate questions and responses, and demonstrate effective nonverbal behavior in an interview and/or one-to-one communication situation

### **ENGL 103: Research and Writing in the Workplace**

Upon completion of this course, a student will be able to:

- Write multiple-page essays and workplace documents that demonstrate critical thinking (including an 8-10 page research paper) that meet high standards for content, organization, style, grammar, mechanics, and format as well as accepted conventions of writing in the workplace
- Write effective, sound, and well-supported arguments using a variety of rhetorical techniques and conventions
- Manage the research and writing process effectively and show evidence of effective planning for research project methods and resource use
- Identify and respond to a range of audiences, including those encountered in a workplace environment, effectively in written and oral assignments
- Formulate a thesis to anchor development of an argument appropriate to audience
- Analyze readings for implied and direct meaning and for tone, audience, and purpose
- Synthesize a variety of viewpoints to develop an individual argument position
- Develop and analyze arguments using logic and other appeals



- Identify flawed logic or logical fallacies
- Participate constructively in discourse that may be controversial in nature, including discourse encountered in collaborative writing groups in the workplace
  - Use computer technology and appropriate software applications to produce documentation, quantitative data presentations, and functional graphical presentations appropriate to various academic and professional settings
- Identify valid issues for research compatible with relevant business purposes and practices
  - Formulate research questions that aid in discovery and analysis
- Use traditional library and online research skills to locate and evaluate college-level research materials as well as types of sources appropriate to research and writing in the workplace
  - Integrate outside information into essays
  - Use appropriate standard documentation procedures
  - Recognize and avoid plagiarism

### **NWIT 203: Windows Server Administration**

Upon completion of this course, a student will be able to:

- Explain the purpose and functions of an operating system and identify different operating systems
- Use the command line to manage a computer system
- Install the Windows operating system, utilize the user interface to issue commands, and run applications
  - Explain files and their location, storage, use, and attributes
- Identify basic concepts and procedures for creating and managing files and directories
  - Do basic disk management including management utilities, backup and recovery, formatting, partitioning, de-fragmentation, and scandisk
- Create batch files

### **NWIT 252: Intermediate Cisco Networking**

Upon completion of this course, a student will be able to:

- Describe different types of WAN connections, encapsulation, and protocols; the difference between a WAN and a LAN and the standards and protocols each uses; which organizations are responsible for WAN standards; the role of a router in a WAN; the physical characteristics of a router; the common ports on a router; the internal components of a router and their functions; and how Ethernet, serial WAN, and console ports are properly connected.
- Describe the steps required to establish a HyperTerminal session; the steps required to log in to a router; how to use the Help feature in the command-line interface (CLI); ways to troubleshoot command errors; the basic operation and features of Cisco IOS Software and methods of troubleshooting it; uses of the show version command; the use of the various router user interfaces and modes, methods

used to establish a CLI session with the router; and commands and steps used to alternate between the user command executive (EXEC) and privileged EXEC modes.

- Describe commands used to name a router; how administrators set passwords on a router; the use of the show commands; the command and steps required to configure a serial interface; the command and steps required to configure an Ethernet interface; how an administrator executes changes to a router; how an administrator saves changes to a router; the command and steps required to configure an interface description; the command and steps required to configure a log-in banner; the command and steps required to configure host tables; the purpose of backup documentation; and the steps for password recovery on a router.
- Describe some of the methods to implement, monitor, and maintain Cisco Discovery Protocol (CDP); how CDP creates a network map of the environment; the commands to disable and troubleshoot CDP; some of the reasons to Telnet remotely to other routers; the commands to verify, disconnect, and suspend a Telnet connection; the forms of alternative connectivity tests; uses of the show cdp neighbors command; how to determine which neighboring devices are connected to which local interfaces; how CDP gathers the neighboring devices, and network address information; and the methods to troubleshoot remote terminal connections.
- Describe the stages of the router boot sequence; how Cisco devices locate and load Cisco IOS Software; what the boot system command is used for; the configuration register values; the methods and processes used to locate Cisco IOS Software; the processes and commands used to create and load a software image and configuration file backup; the Cisco IOS Software naming conventions; what files are used by the Cisco IOS and their functions; the locations of the router of the different file types; what each part of the IOS name represents; the steps and processes to save and restore configuration files using TFTP and copy-and-paste; the steps and commands to load an IOS image using TFTP; the steps and commands to load an IOS image using TFTP; and the steps and commands to load an IOS image using XModem.
- Describe the basic principles of routing; the difference between routed and routing protocols; what interior and exterior protocols are used for in routing; the difference between static versus dynamic routes; how static routes are configured; how default routes are configured; methods for troubleshooting static route configurations; why dynamic routing protocols are necessary; distance vector routing; link-state routing; and how different routing protocols are used in context.
- Describe the steps for initial router configuration; the defining characteristics of RIP; steps and commands to configure a RIP routing scenario; the defining characteristics of IGRP; steps and commands to configure an IGRP routing scenario; load balancing over multiple paths; how routing loops occur in distance vector routing; methods used by distance vector routing protocols to ensure that routing information is accurate; the use of the ip classless command; and methods and techniques to troubleshoot RIP.
- Describe the important uses of ICMP; some of the ICMP error message types and how they are identified; potential causes of specific ICMP error messages and how they are identified; the kinds of ICMP control messages used in networks today; and some of the possible events that can cause ICMP control messages.

- Describe methods of performing basic network testing; methods used to examine the routing table; how the ping command is used to perform basic network connectivity tests; how the telnet command is used to verify the application layer software between source and destination hosts; methods of troubleshooting by testing OSI layers; how the show interfaces command is used to confirm Layer 1 and Layer 2 problems; how the show ip route and show ip protocol commands are used to identify routing issues; how the show cdp command is used to verify Layer 2 connectivity; how the traceroute command is used to identify the path that a packet takes between networks; how the show controller serial command is used to ensure that the proper cable is attached; and how the basic debug command is used to show router activity.
- Describe a positive acknowledgement and retransmission (PAR) and how it relates to TCP; how TCP relates to multiple conversations between hosts, the ports used for services and clients; the well-known ports; the relationship between MAC addresses, IP addresses, and port numbers; the primary functions of TCP, TCP synchronization and flow control; the primary processes and operations of the User Datagram Protocol (UDP); and the common port numbers and what they are used for.
- Describe some of the uses and/or purposes of ACLs; how ACLs provide security and/or control to a network; how to determine which wildcard mask to use; the difference between standard ACLs, extended ACLs, and named ACLs; and ways in which ACLs relate to firewall architecture.

#### **PHIL 140: Introduction to Ethics**

This course covers contemporary ethical issues in public policy and personal conduct. Topic areas may include bioethics and medicine; inequality and discrimination; justice and punishment; information ethics; and environmental ethics among others. Practical issues in these areas will be discussed in relation to ethical theories. Various ethical perspectives will be critically examined.

Upon completion of this course, a student will be able to:

- Demonstrate a comprehension of current moral issues in light of various ethical theories
- Recognize classical thinkers from around the world by exploring normative judgments and foundations for those judgments
- Distinguish normative and non-normative ethical theories and the distinction between meta-ethics and normative ethics
- Critically evaluate different moral points of view, including altruism, universalism, and self-interest
- Discuss different schools of ethical thought

#### **Two examples of Security Specialization Electives offered to BACS students:**

##### **Advanced Digital Forensics and Incident Response**

This in-depth, digital forensics course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks. Situations include

APT adversaries, organized crime syndicates, and hactivism. Students will learn advanced use of a wide range of best-of-breed, open-source tools in the SIFT Workstation to perform incident response and digital forensics; threat hunting techniques that will aid in quicker identification of breaches; rapid incident response analysis and breach assessment; incident response and intrusion forensics methodology; remote and enterprise incident response system analysis; Windows live incident response; memory analysis during incident response and threat hunting; detailed instruction on Windows enterprise credentials and how they are compromised; internal lateral movement analysis and detection; rapid and deep-dive timeline creation and analysis; volume shadow copy exploitation for hunting threats and incident response; detection of anti-forensics and adversary hiding techniques; discovery of unknown malware on a system; adversary threat intelligence development, indicators of compromise, and usage; cyber-kill chain strategies; and step-by-step tactics and procedures to respond to and investigate intrusion cases. Constantly updated ACS 4508 addresses today's incidents by providing hands-on forensics tactics and techniques that elite responders are successfully using in real-world breach cases. ACS 4508 is a substantially extended version of SANS course FOR508, adding in-depth systems and networking knowledge that make a good forensics analyst an even better one.

*Assessment:* GIAC Certified Forensic Analyst (GCFA) examination

### **Security Essentials for Industrial Control Systems**

With the dynamic nature of industrial control systems (ICS), many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle. Students will gain an understanding of ICS components, purposes, deployments, significant drivers, and constraints; use hands-on lab learning experiences to control system attack surfaces, methods, and tools; learn control system approaches to system and network defense architectures and techniques; learn incident-response skills in a control system environment; learn governance models and resources for industrial cybersecurity professionals; and gain an appreciation, understanding, and common language that enables them to work together to secure ICS environments. The course helps develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world. This course is an extended version of SANS course ICS410, adding extensive operating system, networking, hardware, and common exploit modules that will make IT staff much stronger partners for ICS engineers.

*Assessment:* Certified Industrial Cybersecurity Professional (GICSP) examination

**5. Discuss how general education requirements will be met, if applicable.**

BACS students will complete at least 40 hours of general education courses during their BACS program including courses taken at both Montgomery College and STI. Four of those courses will develop and fine-tune their written and oral communication skills, including an intense course on effective cybersecurity writing and speaking. A fifth course will help them understand how ethical considerations may be brought to bear on the choices they make. The remaining courses will ensure that their general education courses meet COMAR requirements.

**6. Identify any specialized accreditation or graduate certification requirements for this program and its students.**

Each student who earns a BACS diploma will have achieved certification in at least five areas of cybersecurity using Global Information Assurance Certifications (GIAC). The three broader GIAC certifications of BACS (GSEC, GCIH and GCIA) are specified by the U.S. Department of Defense under DOD Directives 8570 and 8140 as proof that employees and contractors meet the requirements for employment in the highest levels of Technical Information Assurance roles (levels II, III and specialization, respectively). A fourth BACS-required certification enables students to demonstrate that they are prepared to become cybersecurity tool-builders – one of the most sought-after specialization in the field. The fifth through seventh certifications enable the student to demonstrate competence in specialized areas of cybersecurity that match the needs of firms where they might seek employment, and/or in areas that they want to pursue as their initial specialization in cybersecurity.

**7. If contracting with another institution or non-collegiate organization, provide a copy of the written contract.**

Under a formal Memorandum of Understanding (MOU), STI outsources to SANS (STI's parent organization) many of the operational and administrative functions required to support operations, including establishment of most of our learning environments (physical and virtual), financial transactions, accounting, technology, and other administrative support services. Using this mechanism, STI benefits from SANS's economies of scale and transforms typically high-fixed-cost elements into manageable, smaller variable costs. STI also benefits from its relationship with Global Information Assurance Certification (GIAC), a sister company also owned by SANS. GIAC was established in 1999 to develop and offer exams and certifications that validate whether an individual has gained sufficient competency or mastery of the complex topics taught in SANS courses, and most technical STI courses require students to pass a GIAC certification exam. GIAC exams are the product of broad-based job task analyses that incorporate feedback from hundreds of industry participants. Exam questions and answers and scoring patterns are reviewed and assessed by a PhD in psychometrics. Many of these certification exams have been designed with such a degree of quality that they are, themselves, certified by the American National Standards Institute (ANSI). Thus, learning in STI's BACS courses is validated not by exams created by individual faculty members, but by assessments created by a highly specialized exam creation and testing organization that also keeps these exams current with changing professional requirements over time.

The MOU has enabled all STI degree programs since STI was established and was most recently reviewed and approved during a Middle States accreditation team visit.

A more complete description of the corporate entities, along with the MOUs, is provided in Appendix 2.

**8. Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information on the program.**

STI has a demonstrated record of completeness and transparency in all its academic programs and commits to maintaining a very high level of clarity, thoroughness, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies. You can see evidence of the clarity and completeness of STI's existing undergraduate program at <https://www.sans.edu/academics/undergraduate>

**9. Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.**

We commit to provide only clear and accurate information in our advertising, recruiting, and admissions material. Evidence of the clarity of our advertising and recruiting and admissions information for undergraduate studies may be found at:

<https://www.sans.edu/academics/undergraduate>

**H. Adequacy of Articulation**

Effective articulation agreements are essential to the success of the BACS program because BACS students will complete a large segment of their foundational preparation for STI's advanced cybersecurity courses at Maryland community colleges. For that reason, the BACS program has been designed, from the outset, in cooperation with a Montgomery College team led by MC Germantown Campus Vice President/Provost Margaret Latimer and Academic Cybersecurity Program Manager Joseph Roundy. Course selection for the foundational courses (listed in this proposal) was undertaken in cooperation with Montgomery College to be certain that each course requirement could be met with existing MC resources so as not to put a burden on the college and to allow MC students to transition fully and easily to the STI BACS bachelor degree program.

In addition, STI's President Alan Paller briefed the presidents of Maryland's community colleges at their monthly MCCCCP meeting on October 11, 2019 at Allegany College of Maryland. The president of Allegany College, Cindy Bambara, conducted a follow-up poll of the presidents and reported that 15 of the 16 Maryland community college presidents said they would pursue a joint community college/STI program for a bachelor's degree in cybersecurity. At President Bambara's suggestion, and at the invitation of PGCC Provost Clayton Railey, Mr. Paller briefed the Maryland community college Chief Academic Officers (CAOs) at their December 13, 2019 monthly meeting. The CAOs at the meeting were supportive. The next step is to establish a baseline articulation agreement with Montgomery College and then follow up with the other

interested community college CAOs to adapt the Montgomery College articulation agreement to the courses available at each of the community colleges.

**I. Adequacy of Faculty Resources (outlined in COMAR 13B.02.03.11).**

The members of the BACS faculty are widely respected scholar-practitioners. The faculty serving the students of the proposed BACS program is comprised of the same instructors who currently teach the 700 enrolled graduate students at the SANS Technology Institute as well as the 200 students enrolled in the upper division BACS certificate program. This faculty also teaches the 47,000 students who enroll in SANS non-credit courses each year. Their qualifications to fulfill our mission were recently reviewed and confirmed by the Visiting Team of the Middle States Commission on Higher Education as part of STI's five-year re-accreditation review. Therefore, we believe that our faculty is adequate in both capability and number to serve this new program.

The following is a list of faculty members with credentials and courses taught:

<b>Name</b>	<b>Degree</b>	<b>Field of Degree</b>	<b>Academic Title Rank</b>	<b>Status</b>	<b>Course(s)</b>
Ed Skoudis	MS	Information Networking	Faculty Fellow	Full-time	ACS 3504, ACS 4560
Johannes Ullrich	PhD	Physics	Faculty Fellow, Dean of Research	Full-time	ACS 4401
James Lyne	MS	Information Security	Certified Instructor	Full-time	ACS 2201
Steve Simms	MS	Information Science	Faculty Fellow	3/4 time	ACS 4660, ACS 4760
Keith Palmgren	BS	Information Technology	Certified Instructor	Adjunct	ACS 3301
Alan Paller	MS	Information Systems	President	Full-time	ACS 4023
Lenny Zeltzer	MS	Information Security	Senior Instructor	Adjunct	ACS 4023
Mark Baggett	MS	Information Security Engineering	Senior Instructor	Full-time	ACS 3573
David Hoelzer	MS	Computer Science	Chief Curriculum Faculty Fellow, Dean of Faculty	Full-time	ACS 4503

Many of the STI faculty members are nationally known leaders in cybersecurity, as documented below. Learning from such industry leaders who provide real-world cases for the concepts, tools, and techniques they are teaching helps STI students gain more than academic knowledge – they also develop the confidence to implement what they have learned and the competence to do

it well. Some of the STI faculty members who are directly associated with the courses included in the BACS program are described below.

### **Ed Skoudis, BACS Program Director**

Ed Skoudis has taught cyber incident response and advanced penetration testing techniques to more than 18,000 cybersecurity professionals. He is a SANS Faculty Fellow and the lead for the SANS Penetration Testing Curriculum and SANS Cyber Team Training Curriculum. His courses distill the essence of his own real-world, front-line case studies because he is consistently one of the first experts brought in to provide after-attack analysis on major breaches where credit card and other sensitive financial data are lost. Each year Ed keynotes the RSA conference, the largest conference in the field, along with STI faculty members Johannes Ullrich and Heather Mahalik. Their keynote presents the most dangerous new attacks these experts foresee becoming damaging in the coming year. Ed led the team that built NetWars, the low-cost, widely used cyber training and skills assessment cyber ranges relied upon by military units and corporations with major assets at risk. His team also built CyberCity, the fully authentic urban cyber warfare simulator that was featured on the front page of the *Washington Post*. He was the expert called in by the White House to test the security viability of the Trusted Internet Connection (TIC) that now protects U.S. government networks, and he led the team that first publicly demonstrated significant security flaws in virtual machine technology. He has the rare capability to translate advanced technical knowledge into easy-to-master guidance as demonstrated by the popularity of his step-by-step *Counter Hack* books. Ed earned an M.S. in information networking from Carnegie Mellon University, and a B.S. in electrical engineering from the University of Michigan, summa cum laude.

Ed created and teaches both ACS 4504: Incident Handling and Hacker Exploits and ACS 4560: Network Penetration Testing and Ethical Hacking.

### **Dr. Johannes Ullrich**

Johannes is Dean of Research at STI and also created and manages the SANS Internet Storm Center (ISC) and the GIAC research paper program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and his credits include being named by *Network World* as one of the 50 most powerful people in the networking industry. Johannes holds a PhD in physics from SUNY Albany. His daily podcast, listened to by more than 10,000 professionals, summarizes the latest security threats in a concise format.

Johannes teaches ACS 4503: Intrusion Detection In-Depth and supports STI students in their graduate and undergraduate research initiatives.

### **Rob Lee**

Rob is the chief curriculum director and faculty lead as well as curriculum lead and



author for digital forensic and incident response training at SANS. Rob has more than 18 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations, where he led a team conducting computer crime investigations, incident response, and computer forensics. He worked with the U.S. Department of Defense and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, as lead for a cyber forensics branch, and as lead for a digital forensic and security software development team. Rob was also a director for Mandiant (currently the forensics arm of FireEye), a company focused on investigating advanced adversaries, such as the APT. He is a co-author of the Mandiant threat intelligence report *M-Trends: The Advanced Persistent Threat*. Rob also co-authored the book *Know Your Enemy*. He earned his MBA from Georgetown University.

Rob created and teaches ACS 4508: Advanced Digital Forensics and Incident Response

### **Heather Mahalik**

Heather Mahalik has worked on high-stress and high-profile digital forensics cases, investigating everything from child exploitation to Osama Bin Laden's media. She has helped law enforcement, eDiscovery firms, and the federal government extract and manually decode artifacts used in solving investigations around the world. Heather began working in digital forensics in 2002 and has been focused on mobile forensics since 2010 – there's hardly a device or platform she hasn't researched or examined or a commercial tool she hasn't used. She also maintains [www.smarterforensics.com](http://www.smarterforensics.com), where she blogs and hosts work from the digital forensics community. She is the co-author of [Practical Mobile Forensics](#) (1st and 2nd editions), currently a best seller from Pack't Publishing, and the technical editor for *Learning Android Forensics*.

Heather created and teaches Smartphone Forensic Analysis In-Depth.

### **Stephen Sims**

Stephen Sims is an industry expert with over 15 years of experience performing reverse engineering, exploit development, threat modeling, and penetration testing. He has a MS in information assurance from Norwich University and is a Faculty Fellow for the SANS Institute and author of SANS' only 700-level course, Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP®, CISA, Immunity NOP, and many other certifications.

Stephen teaches ACS 4501: Enterprise Defender.

## **J. Adequacy of Library Resources (outlined in COMAR 13B.02.03.12).**

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that helps STI students and alumni maintain their edge in security. The SANS Resource Center is a compilation of thousands of original research papers, security policies, and security notes, along with a wealth of unique network security data. Supplemented by an online research library subscription and other SANS information services, our current and future students have continuous access to the following list of primary resources:

- The SANS Information Security Reading Room, which contains more than 2,900 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year.
- Free and unlimited access to EBSCO's Computers and Applied Sciences (Complete) database. EBSCO is the leading provider of online research databases, e-journals, magazine subscriptions, e-books, and discovery services of all kinds. This full-text database covers computing, technology, and engineering disciplines, and contains 650 active full-text journals and magazines, 520 active full-text peer-reviewed journals, 320 active full-text peer-reviewed journals with no embargo, and 410 active full-text and indexed journals.
- The SANS Security Policy Collection, which contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Technology Institute's Cyber Research page, which provides access to exemplary graduate-level research papers, group projects, and presentations that cover a wide variety of topics of practical and academic relevance that have real-world impact and often provide cutting-edge advancements to the field of cybersecurity knowledge.
- The SANS Top-20 V7, a consensus list of vulnerabilities that require immediate remediation. The list is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection, which helps keep students up to date with the high-level perspective of the latest security news.
- The Security Glossary, which is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection, which contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at <http://www.sans.org/security-resources/idfaq/>.
- The SANS Internet Storm Center Handler Diaries and Archives, which contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students

with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms and other attacks spread through the Internet.

- SANS Web Briefings held several times a month that feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

#### **K. Adequacy of Physical Facilities, Infrastructure, and Instructional Equipment**

This program will be offered in combinations of three online modalities and in residential institutes. Courses to be offered in the BACS program were available in 2019 at more than 400 residential institutes with a cumulative capacity of more than 40,000 students. Most of the large residential institutes are being reconstituted as live-on-line programs, during the COVID-19 pandemic. We anticipate that a large subset of those residential institutes will be reconstituted as combination face-to-face and live-on-line programs once the pandemic is brought under control.

STI students also have access to the same course delivered live-on-line or on-demand. Those delivery systems currently serve more than 18,000 students each year and have significant capacity for growth. In evidence provided to Middle States Commission on Higher Education for STI's accreditation review, GIAC test results for students who studied using the online modalities were as high as those who studied at the residential institutes. Thus, the instructional infrastructure is capable of supporting 1,000 or more BACS students.

**L. Adequacy of Financial Resources with Documentation (outlined in COMAR 13B.02.03.14)**

1. Complete Table 1: Resources and Table 2: Expenditures . Finance data for the first five years of program implementation are to be entered.
2. Provide a narrative rationale for each of the resource categories.

Table 1: RESOURCES

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	\$1,842,500	\$4,606,250	\$6,909,375	\$9,212,500	\$9,212,500
a. Number of F/T Students	40	100	150	200	200
b. Annual Tuition/Fee Rate	\$17,187.50	\$17,187.50	\$17,187.50	\$17,187.50	\$17,187.50
c. Total F/T Revenue (a x b)	\$687,500	\$1,718,750	\$2,578,125	\$3,437,500	\$3,437,500
d. Number of P/T Students	60	150	225	300	300
e. Credit Hour Rate	\$1,375	\$1,375	\$1,375	\$1,375	\$1,375
f. Annual Credit Hour Rate	14	14	14	14	14
g. Total P/T Revenue (d x e x f)	\$1,155,000	\$2,887,500	\$4,331,250	\$5,775,000	\$5,775,000
3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	\$1,842,500	\$4,606,250	\$6,909,375	\$9,212,500	\$9,212,500

**Finance Data: Narrative**

Table 1: RESOURCES

1. Re-allocated Funds

*Narrative: Analyze the overall impact that the reallocation will have on the institution, particularly on existing programs and organizations units.*

N/A

2. Tuition and Fee Revenue

*Narrative: Describe the rationale for the enrollment projections used to calculate tuition and fee revenue.*

The tuition projection for Year 1 assumes the BACS program admits 40 full-time students who each pay \$34,375 over two years, plus another 60 students who complete the program part-time paying one-half of that same cost over each of four years. We believe this is an appropriate estimate given that we have been able to attract many students to immersion academies in Maryland without the benefit of the public relations and marketing activities that will be associated with the launch of this program.

In each subsequent year, we project that enrollment will progress to 250, then 375, and finally to 500 students completing the BACS program in each of Years 2 – 5, with no planned tuition increases and no change in the percentage of admitted students who will not be responsible for the cost of the program. We believe expectations for significant growth are reasonable because we will be able to expand the offering of the program to students from other states, and because 500 students will still constitute less than 3% of the total number of professionals trained by STI's parent each year.

3. Grants and Contracts

*Narrative: Provide detailed information on the sources of funding. Attach copies of documentation supporting funding. Also, describe alternative methods of continuing to finance the program after outside funds cease to be available.*

N/A

4. Other Sources

*Narrative: Provide detailed information on the sources of the funding, including supporting documentation.*

N/A

5. Total Year

*Narrative: Additional explanation or comments as needed.*

N/A

Table 2: EXPENDITURES

Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	\$737,000	\$1,842,500	\$2,763,750	\$3,685,000	\$3,685,000
a. # Sections offered	N/A	N/A	N/A	N/A	N/A
b. Total Salary	\$442,200	\$1,105,500	\$1,658,250	\$2,221,000	\$2,221,000
c. Total Benefits	\$294,800	\$737,500	\$1,105,500	\$1,464,000	\$1,464,000
2. Admin. Staff (b + c below)	\$168,000	\$420,000	\$672,000	\$840,000	\$840,000
a. # FTE	2	5	8	10	10
b. Total Salary	\$120,000	\$300,000	\$480,000	\$600,000	\$600,000
c. Total Benefits	\$48,000	\$120,000	\$192,000	\$240,000	\$240,000
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	\$45,000	\$73,500	\$76,000	\$77,700	\$77,700
TOTAL (Add 1 – 7)	\$950,000	\$2,336,000	\$3,511,750	\$4,602,700	\$4,602,700

### *Faculty*

BACS students may receive instruction live in-classroom or online, depending on the course and their own choices. When they attend live in-classroom courses, they will be attending a class already being taught by STI faculty to other students. We estimate that this program will represent less than 4% of the total salary and benefits of the faculty involved, because this program is small relative to the total operations of SANS (more than 40,000 students in 2017). When students choose to take the course online, no additional faculty will be required and, similar to live classes, BACS students will represent only a small fraction of those students being taught by the existing group of instructors and teaching assistants. Therefore, we do not anticipate any increase in the number of faculty required to teach BACS students, either live or online, beyond the natural growth of the SANS faculty.

While the costs associated with the faculty who teach these students is embedded in the payments associated with the Memorandum of Understanding between STI and SANS, we have separated out projected amounts for Faculty Salary and Faculty Benefits in Table 2.

#### *Administrative and Support Staff*

The STI graduate programs currently operate at a ratio of students to administrative staff ratio of 150:1 (including both full-time administrative and support staff). Because we anticipate that the students in the BACS program will require more attention, particularly because of their job search and Title IV reimbursement activity, we projected expenses using a more conservative ratio of student to staff of 50:1. Average salary and benefit information is reflective of our current cost experience and market expectations.

#### *Equipment, Library, and New and/or Renovated Space*

The BACS program will not require any additional equipment, library facilities, or any new and/or renovated space. We have ample capacity in our existing facilities, residential institutes, online platform capacity, and offices.

#### *Other Expenses*

As described elsewhere, a core design element of the SANS Technology Institute is the Memoranda of Understanding signed with our parent, the SANS Institute, and a related entity, GIAC Corporation, that allow STI to select and pay for many costs on a variable, per-student basis. The BACS program will also benefit from this financial arrangement. The financial projections assume the same mix of payments that STI incurs today per student, as recently reviewed by the Middle States Evaluation Team during our re-accreditation study.



**M. Adequacy of Provisions for Evaluation of the Program (outlined in COMAR 13B.02.03.15).**

Continuous, closed-loop evaluation has been the hallmark of STI programs since the institute was established. STI employs a three-level evaluation program completely embedded in the curriculum. The 2018 Middle States Evaluation Team commended this evaluation methodology: “SANS Technology Institute should be commended for the fact that its curriculum automatically embraces learning outcomes and program outcomes.”

1. *Every day, in every STI class, every student is expected to complete an evaluation of the teaching effectiveness, currency, and value of the course material, and the quality of the labs, exercises, and other aspects of their learning experience.* Their forms are processed by an evaluation team and results are delivered by 11:30 that evening to STI’s president and senior staff. The evaluation team follows up on all strong concerns and, in cases in the past when a faculty member was clearly struggling, has replaced the teacher by noon the next day based on the evaluations. In addition, the evaluation team compiles and feeds course content suggestions or concerns to the course author for consideration or inclusion in the annual (or sometimes more frequent) course updates. Data on labs or other technology go to the appropriate teams for continuous or major product improvement. This evaluation system is also used in vLive and Simulcast distributed learning modalities. For On-Demand, the evaluation cycle is based on module completion rather than days, but the system functions identically and in fact responses are easier to process because entries are already in digital form when submitted.

2. *Evaluation of course-level student outcomes uses reliable measures of mastery, not subject to variability, that are associated with individual faculty members’ understanding of the course outcomes.* Each course has an associated examination that is recognized as a widely accepted and valued way to validate mastery of the course outcomes. For example, all BACS students will be required to complete a course in which they learn incident handling techniques, common attack techniques, and the most effective methods to stop intruders using those attack techniques. The exam and certification associated with this course is called the Global Cybersecurity Incident Handler (GCIH) test and certification. The value of this exam is demonstrated by the fact that each year employers pay for more than 9,000 of their employees and job candidates to take this course and sit for the GCIH exam (pass rate of approximately 79%). The acceptance of the exam is validated by the U.S. Department of Defense (DoD) directive that names GCIH certification as proof that a DoD employee or contractor is capable of taking on the highest of three levels of technical cybersecurity roles in DoD. The GIAC certifications used for evaluating student mastery of course objectives are updated using a large-scale job-task analysis that interviews practitioners at least every three years. This process, along with the psychometric assessments that shape question assessment, is subject to regular review by the American National Standards Institute. GIAC exams increasingly include hands-on test questions where students can demonstrate they can use what they learned.

3. *To evaluate program outcomes, STI tracks all graduates and asks them (and when possible, their employers) annually for feedback on how well the program worked for them and how it might be improved.*

This three-level closed-loop assessment system has led to the extraordinary success of STI graduates and their substantial impact on major organizations, as documented in Appendix 3.

**N. Consistency with the State’s Minority Student Achievement Goals (outlined in COMAR 13B.02.03.05 and in the State Plan for Postsecondary Education).**

Strategy 4 of the Maryland State Plan calls for collaboration between historically black universities and colleges (HBUCs) and other institutions to ensure equal educational opportunity for all Marylanders. To identify students who will excel in the BACS program, SANS will use the CyberStart talent identification simulator that allows people who have never worked in IT to discover whether they would be good at cybersecurity and like it. We will use the simulator in all Maryland community colleges that choose to participate and also make the same gamified simulation available to students in HBCUs that choose to be partners, and we will follow up with additional support for the HBCUs to help their talented students pursue further study in cybersecurity and its foundations. The simulator and evidence of its reliability are further described in Section B.2 above, **Alignment with the 2017–2021 Maryland State Plan for Postsecondary Education.**

**O. Relationship to Low-productivity Programs Identified by the Commission**

N/A

**P. If Proposing a Distance Education Program, Please Provide Evidence of the Principles of Good Practice (outlined in COMAR 13B.02.03.22C).**

See Appendix 4 for the evidence that this program complies with the Principles of Good Practice.

## **Appendix 1. Letters from Employers Ready to Interview and Hire Students Who Complete the Courses and Certifications of the BACS Program**

New commitments exclusively for BACS:

- Minerva Engineering
- Native American Engineering Solutions

Commitments for the Maryland EARN program with two GIAC Certifications (BACS graduates earn 5 GIAC Certifications)

- Defense Point Security
- GEICO
- CACI
- Thermo Fisher
- Spry Methods
- Aerstone
- PLEX Solutions
- RBR Technologies
- IntelliDyne
- Halfaker
- NTT Solutions



A Certified  
Service-Disabled  
Veteran-Owned  
Small Business

# Minerva Engineering

Harden • Defend • Secure

7250 Parkway Drive Suite 100 Hanover, MD 21076

Max Shuftan  
SANS Institute

May 14, 2020

Subject: Letter of Commitment

Dear SANS Technology Institute:

The intent of this Letter is to provide an expression of support of MINERVA ENGINEERING to be an employer partner of the SANS Technology Institute's Strategic Industry Partnership (SIP) for the Bachelor of Professional Practice in Applied Cybersecurity (BACS). BACS is an undergraduate 4-year degree program in which each graduate will complete at least 5 advanced SANS cybersecurity courses and their corresponding GIAC certifications, as well as training in effective security writing and presentation.

As an employer partner of this BACS SIP, MINERVA ENGINEERING commits to hiring consideration of the graduates of the SANS BACS program. This Letter does not guarantee that Employer will execute any hires of graduates. MINERVA ENGINEERING hires approximately 20-40 cybersecurity professionals each year and based on the training and certifications to be earned by graduates in the BACS, believes the program would produce skilled candidates for hiring consideration.

Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Digitally signed by Donald W.  
Holmes:AO1097C000015C3CBF446700002CD3  
DN: c=US, o=U.S. Government, ou=ECA,  
ou=IdenTrust, ou=Minerva Engineering, cn=Donald  
W. Holmes:AO1097C000015C3CBF446700002CD3  
Date: 2020.05.14 13:36:56 -0400

Donald W. Holmes, CEO



### **LETTER OF COMMITMENT**

Native American Industrial Solutions LLC (NAIS)  
14323 Ocean Highway Suite 4119  
Pawleys Island SC 29585

Dear SANS Technology Institute:


The intent of this Letter is to provide an expression of support of NAIS to be an employer partner of the SANS Technology Institute's Strategic Industry Partnership (SIP) for the Bachelor of Professional Practice in Applied Cybersecurity (BACS). BACS is an undergraduate 4-year degree program in which each graduate will complete at least 5 advanced SANS cybersecurity courses and their corresponding GIAC certifications, as well as training in effective security writing and presentation.

As an employer partner of this BACS SIP, NAIS commits to hiring consideration of the graduates of the SANS BACS program. This Letter does not guarantee that Employer will execute any hires of graduates. NAIS hires approximately 25 cybersecurity professionals each year and based on the training and certifications to be earned by graduates in the BACS, believes the program would produce skilled candidates for hiring consideration.

Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jeremy Meyers, PhD  
President & CEO, NAIS

 Date: 12 May 2020



**LETTER OF COMMITMENT**

**DEFENSE POINT SECURITY, LLC  
44 CANAL CENTER PLAZA, SUITE 305  
ALEXANDRIA, VA 22314**

**Dear SANS Institute:**

The intent of this Letter is to provide a written expression of commitment of Defense Point Security, LLC to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, Defense Point Security, LLC commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. Defense Point Security, LLC hires approximately 54 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

**Dave Poole, Chief Operating Officer  
Defense Point Security, LLC**

DocuSigned by:  
  
Date: 8/24/2017



**LETTER OF COMMITMENT**

**GEICO**  
**1 GEICO Plaza**  
**Washington DC. 20076**

**Dear SANS Institute:**

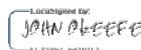
The intent of this Letter is to provide a written expression of commitment of GEICO to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. GEICO's sole obligation on as an employer partner of this EARN MD SIP, means that GEICO commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy") who apply for employment with GEICO. All provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates.

The SANS Institute understands that they may not issue any press releases or use GEICO's trademarks for any advertising, marketing or promotional purposes, or in any form on the Internet, without the express prior written consent of GEICO. Use of the "GEICO" name in mass release emails is strictly prohibited. Except as set forth in this paragraph, the SANS Institute shall not, under any circumstances, use, display, publish or distribute GEICO's name or trademarks, without the express written permission of GEICO.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

**John OKeefe, CISO & Infrastructure AVP**  
**GEICO**

A handwritten signature in blue ink that reads "JOHN O'KEEFE". Above the signature, there is a small, faint stamp that says "LOCKED SIGNATURE". Below the signature, there is a small, faint stamp that says "11/11/2017 10:40AM".

**Date:** September 12, 2017



**LETTER OF COMMITMENT**

???

?

CACI NSS, Inc.  
11955 Freedom Drive  
Reston, VA 20190

?

Dear SANS Institute:

?

The intent of this letter is to provide a written expression of commitment of CACI NSS, Inc. (CACI) to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries Grant Solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, CACI commits to consider hiring the graduates of the SANS Institute's proposed Cyber Talent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This letter does not guarantee that Employer will execute any hires of Academy graduates. CACI hires approximately 75-125 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

???

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to withdrawal and modification at any time without incurring any legal liability or obligation.

???

Sincerely,

?

?

Calvin Freeman  
Executive Director, Procurement  
CACI NSS, Inc.

?

?

Date: 9/8/2017

?

CACI International Inc. and Subsidiary Companies  
CACI, INC. – FEDERAL  
14370 Newbrook Drive, Bldg. A, Chantilly, Virginia 20151 - (703) 679-3100 - FAX (703) 679-3184  
CACI Website – <http://caci.com>

Washington, D.C. – La Jolla – London





LETTER OF COMMITMENT

Thermo Fisher Scientific  
168 3<sup>rd</sup> Ave.  
Waltham, MA 02451

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Thermo Fisher Scientific to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, Thermo Fisher Scientific commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. Thermo Fisher Scientific hires approximately 20 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Laura Butler, Sr. Manager/ Talent Acquisition  
Thermo Fisher Scientific

 Date: 9/8/2017



**LETTER OF COMMITMENT**

Spry Methods  
1420 Spring Hill Rd, Suite 300  
McLean, VA 22102

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Spry Methods to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) for the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant that will be implemented in 2018-2019. As an employer partner of this EARN MD SIP, Spry Methods commits to hiring consideration of the graduates of the SANS Cyber Workforce Academy ("Academy"). This Letter does not guarantee that Employer will execute any hires of Academy graduates. Spry Methods hires approximately 20 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates for hiring consideration.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. The provisions in this Letter of Commitment are nonbinding. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jason Gebert, Program Manager  
Spry Methods

A handwritten signature in black ink, appearing to read "Jason Gebert", written over a horizontal line.

Date: 2/2/2018



Quest Consultants LLC  
DBA Aerstone  
12250 Rockville Pike  
Suite 250  
Rockville MD 20852

**LETTER OF COMMITMENT**

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Aerstone to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) for the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant that will be implemented in 2018-2019. As an employer partner of this EARN MD SIP, Aerstone commits to hiring consideration of the graduates of the SANS Cyber Workforce Academy ("Academy"). This Letter does not guarantee that Employer will execute any hires of Academy graduates. Aerstone hires approximately 4 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates for hiring consideration.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. The provisions in this Letter of Commitment are nonbinding. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Francis W Schugar  
Quest Consultants LLC DBA Aerstone

*Francis W Schugar*

Date: 01/30/2018

Aerstone  
12250 Rockville Pike suite 250, Rockville MD 20852



LETTER OF COMMITMENT

PLEX Solutions, LLC  
Wisconsin Ave  
Bethesda, MD 20814 United States

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of PLEX Solutions, LLC to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, PLEX Solutions, LLC commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. PLEX Solutions, LLC hires approximately 20 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without incurring any legal liability or obligation.

Sincerely,

Adam Nielson, Senior Information Assurance Expert  
PLEX Solutions, LLC

 Date: 9/8/2017



### LETTER OF COMMITMENT

RBR-Technologies, Inc.  
2288 Blue Water Blvd  
Suite 322  
Odenton, MD 21113

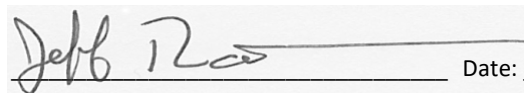
Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of RBR-Technologies, Inc. to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, RBR-Technologies, Inc. commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. RBR-Technologies, Inc. hires approximately 5 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest. The cybersecurity roles RBR-Technologies, Inc. focus on include Information Systems Security Engineers, Security Intel Analysts, Cyber Network Defense Operators, which all require extensive training in order to possess the appropriate skill sets to be successful.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jeff Rathmann, Chief Technology Officer  
RBR-Technologies, Inc.

 Date: 08/26/2017



**LETTER OF COMMITMENT**

IntelliDyne, LLC  
2677 Prosperity Avenue, Suite 301  
Fairfax, VA 22031

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of IntelliDyne to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, IntelliDyne commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. IntelliDyne hires approximately 3 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Marisa Krafsig  
Sr. HR Director  
IntelliDyne, LLC

Date: 9/5/17



#### LETTER OF COMMITMENT

Halfaker & Associates, LLC  
2900 S Quincy St #410  
Arlington, VA 22206

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Halfaker & Associates, LLC to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) for the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant being implemented in 2018-2019. As an employer partner of this EARN MD SIP, Halfaker & Associates, LLC commits to hiring consideration of the graduates of the SANS Cyber Workforce Academy -Maryland ("Academy"). This Letter does not guarantee that Employer will execute any hires of Academy graduates. Halfaker & Associates, LLC hires approximately 10-12 cybersecurity professionals each year and based on the training and certifications to be earned by graduates in the Academy, believes the program would produce skilled candidates for hiring consideration.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. The provisions in this Letter of Commitment are nonbinding. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jody Naleppa, Executive Vice President  
Halfaker & Associates, LLC

A handwritten signature in black ink that reads "Jody Naleppa".

Date: 03/16/18



NTT Security (US) Inc  
9420 Underwood Avenue  
Omaha, NE 68114  
T +1 866.333.2133  
www.nttsecurity.com

**LETTER OF COMMITMENT**

NTT Security, US  
9420 Underwood Avenue  
Omaha, NE 68114

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of NTT Security, US to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, NTT Security, US commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. NTT Security, US hires approximately 75 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Arlin Halstead, Director Human Resources, US  
NTT Security, US

 Date: 9/8/17



## Appendix 2. Contracts with Related Entities

The SANS Technology Institute (STI) as an educational institution is an independent yet symbiotic and related entity to the much larger SANS and GIAC organizations. As such, it represents a unique integration of existing and purpose-built educational elements from SANS and GIAC, augmented with additional elements that are specific to STI:

- **STI as an independent subsidiary** – STI is an independent but wholly owned subsidiary of SANS, with its own board and administrative staff. As an organization, it is designed to include those full-time personnel who directly serve the admissions and ongoing management and educational servicing of students, while outsourcing most other functions to SANS and GIAC, which operate at scale and may deliver those services (including human resources, finance, and technology systems) to STI at levels or costs that would otherwise be unachievable by an institution with fewer than 1,000 students. This unique combination of dedicated staff and flexible access to world-class scale and quality systems is a key enabler for STI's students to access world-class faculty and educational content from an otherwise small institution.
- **STI's faculty come from SANS** – STI's faculty is comprised of and appointed from the 85 individuals who have achieved the status of being "SANS Certified Instructors," an industry-recognized demarcation of technical achievement practiced in the field, superior teaching effectiveness, capacity to engage students as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities. Among the faculty are people who are called upon to investigate attacks on the
- U.S. government and the country's largest commercial enterprises, who are entrusted to teach practitioners of cybersecurity at the highest and most sensitive (classified) levels, and who through their professional practice and research advance our understanding of cyber threats and potential remediation, and then transmit that knowledge forward to our students and the larger community. Even beyond their superlative technical abilities, our faculty members have skills as teachers that truly set them apart and allow them to impart sometimes dense technical lessons with enthusiasm, applicable real-world examples, and charismatic engagement. While a handful of faculty members serve in full-time teaching and research roles, most are scholar-practitioners who teach less than full-time for the school so that they can engage in the practice of cybersecurity, keep their skills advanced and current, and feed their experiences and learning back into the courses and class discussions.
- **STI's programs designed by STI faculty** – STI's academic programs were designed by the faculty in order to optimally achieve their stated learning outcomes. For each program, the faculty responsible for program design built out the educational content from three distinct sources:
  - **SANS Technical and Management Courses** – SANS maintains the world's largest and most-respected catalog of 36-50 seat-hour courses in cybersecurity, ranging from broad survey courses in cyber defense to highly advanced and specialized penetration testing and digital forensics courses. Each program includes a subset of SANS courses relevant to achieving that program's learning outcomes, including the availability of elective courses. In addition, STI students may avail themselves of all the opportunities at different times and locations throughout the United States (and world) that the courses are offered live and taught by STI faculty, or they may also take the opportunity to take the very same course presented online by SANS, which transforms the best live performance by an STI

faculty member into the online version of the course, complete with the same labs and access to subject-matter experts online. STI thereby offers an extraordinarily broad set of choices for students to tailor their program schedule to fit within their work and personal lives.

- **GIAC Certification Exams** – STI’s faculty deploy various world-class, industry- proven GIAC examinations to validate the learning achieved by each student in a SANS technical course. GIAC exams result from an exam development effort that far exceeds the typical requirements for college-level examinations. That effort includes job task analyses to ensure relevance and psychometric reviews that in turn ensure appropriate difficulty and rigor. Many of the GIAC exams deployed in STI’s programs are themselves ANSI-certified for quality and robustness. The use of those exams enables STI’s programs to ensure that students are assessed fairly and that their performance and grades are constantly level-set against the performance of other industry professionals taking the same exam.
- **STI-specific educational elements and courses** – STI’s faculty creates many additional elements to augment the programs with written security memos and research, oral presentations, group projects, and other experiences designed to require high-level integrations of learning.

Two Memoranda of Understanding (MOU) define the business relationships between STI, its SANS parent, and its sister organization the Global Information Assurance Certification (GIAC) organization. Those MOUs are reproduced in full below.

***Memorandum of Understanding***  
***between***  
**The SANS Technology Institute (“STI”)**  
***and***  
**The Escal Institute of Advanced Technologies**  
**(“SANS”)**

**Agreement Published Date: January 1<sup>st</sup>, 2018**

**Agreement Period of Performance: January 1<sup>st</sup>, 2018 – December 31<sup>st</sup>, 2025**

## **Purpose**

The purpose of this Memorandum of Understanding (“MOU”) is to establish a cooperative partnership between the SANS Technology Institute (STI) and the ESCAL Institute of Advanced Technologies, Inc/dba/SANS Institute (SANS). This MOU will:

- outline services to be offered by SANS to STI;
- quantify and measure service level expectations, where appropriate;
- outline the potential methods used to measure the quality of service provided;
- define mutual requirements and expectations for critical processes and overall performance;
- strengthen communication between the provider of administrative services (SANS) and its enterprise customer (STI);
- provide a vehicle for resolving conflicts.

## **Vision**

SANS will provide a shared business environment for the STI enterprise. The business environment will continuously enhance service, compliance and productivity to STI’s employees, students and core administrative practices. The primary goals for the MOU include:

- **Integrate** people, processes, and technology to provide a balanced service level to all customers. Create a collaborative environment where trusted relationships and teamwork are encouraged between administrative services, departmental staff, faculty, students and suppliers to further the enterprise’s goals.
- **Leverage** human resources, institutional knowledge, developing skill sets, and technology in an effort to continuously improve service and productivity for all services provided. Create an organizational structure that balances STI’s strategic and tactical efforts to promote efficiencies.
- **Mitigate** risk to the STI enterprise by focusing on compliance requirements and understanding the impact these requirements have on productivity and student services. Develop an integrated organizational structure that will promote the consistent interpretation and enforcement of policies, procedures, local, state and federal laws and regulations throughout the enterprise.

## **Mission**

Through various SANS educational and administrative service units, provide business activities dedicated to operational and student service excellence to the STI enterprise so that core STI staff can focus on the academic components of their mission to educate managers of information security groups and technical leaders who direct information security programs.

## Scope

The SANS Institute will provide access for STI students, in all delivery modalities, to the Technical courses offered by the SANS Institute that are a part of STI's course curricula, including, Course Maintenance, Presentation of this course material, and Educational Residency services for the SANS Technology Institute. The SANS Institute shall provide policy-compliant management of Accounting & Finance, Bursar & Registration, Human Resource, Marketing, and Information Technology infrastructures for STI.

## Hours of Operations

Typical staffed hours of operation for the SANS activities are 9:00 – 5:00 Monday-Friday, with the exception of approved holidays. Working hours may be adjusted due to system/power outages, emergency situations, or disaster. Through the use of technology, it is expected that many of the services provided will be available to STI students and employees on a 24-hour basis.

## Service Expectations

SANS and STI agree to the service expectations and working assumptions listed below. These service expectations are meant to monitor the more critical elements of the services provided and are not meant to reflect the comprehensive services offered by SANS. The productivity indicators reflected below are not listed in any order of priority.

## Accounting and Finance

Process	Service Expectation	Service Metric
Accounts Receivable	Remittances produced in the form of check, EFT, or wire.	Payment schedule is set up for a daily cycle and reporting available daily.
Payment accuracy	All payments made will be for approved and legitimate services/products	Audits of vendor transactions will show evidence of 100% three-way match.
Employee travel and expenses are reimbursed.	Protect financial outlays made by employees.	Reimbursements are made within a 30-day timeframe.
Financial reporting	Financial reporting is done on time and in accordance with the same audited accounting principles used by SANS.	All MSCHE, federal and internal reporting deadlines will be met on time.
Audit of records	Annual audits will be performed	Annual audit performed on the Financial Statements by an independent external auditor

## Bursar & Registration

Process	Service Expectation	Service Metric
---------	---------------------	----------------

Cashier Function	Process payments and distribute revenue to appropriate departments	Payments will be processed within 24 hours of receipt, and revenue distributed on a monthly basis
------------------	--	---

## Human Resources

<b>Process</b>	<b>Service Expectation</b>	<b>Service Metric</b>
Benefits	Provide benefits which are in the best interest of the employees and employer	Annual survey of employees will show that major benefits of interest are being adequately provided
Payroll	Assure timely payroll and employee reviews	All bimonthly payrolls will be made on the 15 <sup>th</sup> and final days of the month
HR services	Manage HR service to ensure receipt by employees	HR services are provided for in a timely manner as measure in annual survey and changes are communicated and enforced

## Marketing

<b>Process</b>	<b>Service Expectation</b>	<b>Service Metric</b>
Brand Awareness	Create awareness of STI programs within the information Security Community	SANS will facilitate access to its customer list and will routinely conduct cross- branding to assist with market awareness of STI graduate programs
Technical Expertise	SANS will provide the creative content assistance, graphic editing, and industry expertise required to allow for the execution of STI recruitment campaigns	Generalized STI marketing campaigns are made operational via the availability of a centralized SANS marketing staff

## Information Technology

<b>Process</b>	<b>Service Expectation</b>	<b>Service Metric</b>
Digital learning environment	Create and maintain a leading edge digital environment for learners	Learner surveys consistently scoring above 4 on a scale from 1 to 5, plus recommender percentage greater than 90%.
Technology infrastructure	Provide transaction platforms to support student course registration and other services	Annual surveys of students to reflect adequacy of transaction processes

## Technical Course Maintenance & Presentation

<b>Process</b>	<b>Service Expectation</b>	<b>Service Metric</b>
Currency of content	Make available for use by STI Faculty any and all technical content developed by the SANS Institute	Content is reviewed at least semi-annually for currency with existing malicious capabilities and mitigation theory and strategy

Quality of content and presentations	Assist through all means necessary and available the delivery of STI faculty and lab instruction in a high-quality fashion	SANS Institute will make available all performance ratings derived from students on STI courses or faculty
--------------------------------------	--	--

## Educational Residency

Process	Service Expectation	Service Metric
Conference services	Provide hotel, classroom technology, refreshment and other services that promote an unencumbered learning environment for students	Conference services provided will maintain an average rating of at least 4 out of 5 on daily student surveys

## Service Constraints

- **Workload** - Increases in workload, such as back log due to power outages or fiscal year end closing, may result in temporary reduction of service level delivery.
- **Conformance Requirements** - Finance policy changes and Internal Revenue regulations may alter procedures and service delivery timeframes.
- **Dependencies** - Achievement of the service level commitment is dependent upon student and employee compliance with the policies and procedures of the STI enterprise.

## Terms of Agreement

The term of this agreement is January 1, 2018 - December 31, 2025. This Agreement may be cancelled only by STI, at its sole discretion.

## Periodic Quality Reviews

STI and SANS will jointly conduct periodic reviews of individual SANS administrative support unit performance against agreed-upon service level expectations. The agenda for these reviews should include, but is not limited to:

- service delivery since the last review
- major deviations from service levels
- conflicts or concerns about service delivery
- planned changes to improve service effectiveness
- provide feedback from student and employees
- annual customer satisfaction surveys

STI and SANS will also regularly assess customer satisfaction and will use the results as a basis for changes to this Agreement.

STI's Executive Director and the SANS administrative service unit lead will meet annually.

### **Service Level Maintenance**

This Agreement will be reviewed on an ongoing basis and updated as needed. Revisions may become necessary due to changing service needs, modifications to existing services, addition of services, significant variations from agreed upon-service levels, or unanticipated events.

### **Issue Resolution**

If either party identifies a substantive breach of responsibility, or other problem that requires resolution prior to the next periodic review, the operating level managers of both parties will engage in a joint effort of understanding and rectification of the issue. In the event this remedial effort fails, either party can raise the issue to the executive levels of both parties.

### **Payment Terms and Conditions**

For services provided, STI will pay SANS according to the following schedule:

- STI will pay SANS \$1,500 for each instance when an STI student registers for a full SANS class as part of an STI course, regardless of the chosen delivery modality (live event or online), and as subject to the schedule found at Appendix A for partial or non- standard classes which comprise only 1-credit events within the STI curriculum.
- STI will pay amounts to SANS, monthly in arrears, to reflect any directly allocated expenses by SANS personnel in support of STI business according to this services agreement (specifically including the result of any time allocation procedures as determined by SANS accounting department)
- STI will pay an amount to SANS, monthly in arrears, to reflect its pro-rata share of SANS' otherwise unallocated costs for Accounting & Finance, Bursar, Human Resource, Marketing and Information Technology, and related administrative services, in proportion to its share of revenue relative to SANS revenue also sharing in this services pool.

Agreed to on behalf of STI:

Eric A. Patterson  
Executive Director  
SANS Technology Institute

\_\_\_\_\_  
Date:

Agreed to on behalf of SANS:

Peggy Logue  
Chief Financial Officer  
SANS Institute

\_\_\_\_\_  
Date:



Appendix A: Schedule of SANS Courses Subject to, or Exempt From, the Payment Terms Described in this Agreement

STI Course	SANS Course	Payment Amount
ISE 5101	SEC 401	\$1,500
ISM 5101	MGT 512	\$1,500
ISE/M 5201	SEC 504	\$1,500
ISE/M 5300	MGT 433	\$ 500
ISM 5400	MGT 514	\$1,500
ISE 5401	SEC 503	\$1,500
ISE/M 5500	N/A	\$ 0
ISE 5600	MGT 514 (Day 4)	\$ 500
ISM 5601	LEG 523	\$1,500
ISE/M 5700	N/A	\$ 0
ISE/M 5800	MGT 525	\$1,500
ISE/M 5900	N/A	\$ 0
ISE/M 6001	SEC 566	\$1,500
ISE/M 6100	N/A	\$ 0
ISM 6201	AUD 507	\$1,500
ISE/M 6215	SEC 501	\$1,500
ISE 6230	SEC 505	\$1,500
ISE 6235	SEC 506	\$1,500
ISE 6240	SEC 511	\$1,500
ISE/M 6300	NetWars Cont	\$ 0
ISE 6315	SEC 542	\$1,500
ISE 6320	SEC 560	\$1,500
ISE 6325	SEC 575	\$1,500
ISE 6330	SEC 617	\$1,500
ISE 6350	SEC 573	\$1,500
ISE 6360	SEC 660	\$1,500
ISE 6400	DFIR NetWars Cont	\$ 0
ISE 6420	FOR 500	\$1,500
ISE 6425	FOR 508	\$1,500
ISE 6440	FOR 572	\$1,500
ISE 6450	FOR 585	\$1,500
ISE 6460	FOR 610	\$1,500
ISE 6515	ICS 410	\$1,500
ISE 6520	ICS 515	\$1,500
ISE 6615	DEV 522	\$1,500
ISE 6715	AUD 507	\$1,500
ISE 6720	LEG 523	\$1,500
RES 5500	N/A	\$ 0
RES5900	N/A	\$ 0

# **SANS Technology Institute- GIAC Memorandum of Understanding**

**Agreement Published Date: January 1, 2018**

**Agreement Period of Performance: January 1<sup>st</sup>, 2018 –  
December 31<sup>st</sup>, 2025**

# Contents

## Purpose

This Memorandum of Understanding (“MOU”) revises and supersedes any previously signed agreement between the SANS Technology Institute (STI) and Global Information Assurance Certification (GIAC). This MOU:

- outlines services to be offered and working assumptions between STI and GIAC;
- quantifies and measures service level expectations;
- outlines the potential methods used to measure the quality of service provided;
- defines mutual requirements and expectations for critical processes and overall performance;
- strengthens communication between the provider of assessment services (GIAC) and its enterprise customer (STI);
- provides a vehicle for resolving conflicts.

## Vision

GIAC will provide student assessment services for the STI enterprise. The primary goals for the MOU include:

- **Provide** access to high quality services for students, community and faculty, while ensuring identity and examination integrity in a secure and test-friendly environment.
- **Provide** meaningful certification services to students while promoting their academic, career and personal goals.
- **Demonstrate** that STI students can contribute to the knowledge base in information security and can communicate that knowledge to key communities of interest in information security.

## Mission

Through various service units, GIAC provides assessment activities dedicated to operational and student service excellence to the STI enterprise so that core STI staff can focus on the academic components of their mission to educate managers of information security groups and technical leaders who direct information security programs.

## Scope

GIAC shall provide job task analysis-based assessments in the form of proctored certification exams.

## Hours of Operations

Through the use of technology and GIAC directed service providers, it is expected that assessment services provided will be available to STI students on a 24-hour basis.

## **Service Expectations**

STI and GIAC agree to the service expectations and working assumptions listed below. These service expectations are meant to monitor the more critical elements of the services provided and are not meant to reflect the comprehensive services offered by GIAC. The productivity indicators reflected below are not listed in any order of priority.

## **Service Constraints**

- ***Scheduling of Capstone Examinations*** - The scheduling of the capstone GSE and GSM examinations will occur in conjunction with appropriate STI administrative staff and will adequately account for the number of students requiring a given capstone examination during each year.
- ***Conformance Requirements*** - ANSI policy changes may alter procedures and service delivery timeframes.
- ***Dependencies*** - Achievement of the service level commitment is dependent upon student and faculty compliance with the policies and procedures of GIAC.

## **Terms of Agreement**

The term of this agreement is January 1, 2018 - December 31, 2025. This Agreement may be cancelled only by STI, at its sole discretion.

## **Periodic Quality Reviews**

STI and GIAC will jointly conduct periodic reviews of individual GIAC assessment unit performance against agreed-upon service level expectations. The agenda for these reviews should include, but is not limited to:

- service delivery since the last review
- major deviations from service levels
- conflicts or concerns about service delivery
- planned changes to improve service effectiveness
- provide feedback from student and employees
- annual customer satisfaction surveys

STI and GIAC will also regularly assess customer satisfaction and will use the results as a basis for changes to this Agreement.

STI's Executive Director and the Director of GIAC will meet annually.

## **Service Level Maintenance**

This Agreement will be reviewed on an ongoing basis and updated as needed. Revisions may become necessary due to changing service needs, modifications to existing services, addition of services, significant variations from agreed upon-service levels, or unanticipated events.

## **Issue Resolution**

☐ If either party identifies a substantive breach of responsibility, or other problem that requires resolution prior to the next periodic review, the operating level managers of both parties will engage in a joint effort of understanding and rectification of the issue. In the event this remedial effort fails, either party can raise the issue to the executive levels of both parties.

## **Payment Terms and Conditions**

For services provided, STI will pay GIAC according to the following schedule:

☐ STI will pay GIAC \$325 each time a student pays for a GIAC exam as part of their program of studies, or when they pay tuition or pay for credit hours for a course in which they will take a GIAC certification exam.

☐ STI will specifically pay GIAC \$1000 each time a student pays for a GSE or GSM exam as part of their program of studies.

Agreed to on behalf of STI:

Agreed to on behalf of GIAC:

Eric A. Patterson  
Executive Director  
SANS Technology Institute

Scott Cassity  
Executive Director  
GIAC

Date

Date

### **Appendix 3. Evidence of Compliance with the Principles of Good Practice (outlined in COMAR 13B02.03.22C)**

The proposed program uses the same combination of live classroom and three distance learning modalities used in the STI graduate program that was commended for its “creative and forward looking teaching methodology” in the April 2018 Team Report to the Middle States Commission on Higher Education. That report also noted that all modalities resulted in equivalent scores, with the distance learning modalities earning slightly higher scores in several tougher courses where students needed more time to absorb (and review) the material.

The three distance learning modalities available to students to complete the SANS technical course component are OnDemand, vLive, and Simulcast. Students who use the OnDemand platform are given access to a learning management system with modules pre-loaded into the system and are also provided with printed course books containing written lectures and labs. Each module is a recording from an in-person course session. The learning management system allows students to revisit lectures and also complete quizzes to verify understanding. A recommended viewing schedule is included in course syllabi. Each STI course has a responsible faculty member who in most cases is the same person recorded for the OnDemand course system. A teaching assistant referred to as a virtual mentor is available for all OnDemand courses to help answer student questions or assist with lab issues.

The vLive learning modality is conducted online with established course meeting times led by an instructor – typically twice per week for up to eight weeks – through a learning management system that allows for direct interaction with the instructor and other course participants. Each course session is recorded for students to review previously covered material, or to view if they miss a session.

The Simulcast delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time the in-person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member assigned to the STI course reviews student performance on exams and papers and assigns a grade at the end of the course.

#### **(a) Curriculum and instruction**

##### **(i) A distance education program shall be established and overseen by qualified faculty.**

When implemented for distance education, the courses are converted from the live in-class courses in consultation with and under the direction of the faculty,

**(ii) A program’s curriculum shall be coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.**

If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member who oversees the STI course reviews student performance on exams and papers and assigns a grade at the end of the course. Moreover, the outcomes achieved by students employing STI’s distance learning modalities are demonstrably equivalent to those achieved by students who attend live in-person courses.

The Working Group for the 2014 Substantive Change Request, whereby STI was approved by Middle States to deliver more than 50 percent of our credit via distance modalities, reported:

“A 2013 study of all certification exam results provided evidence that the exam scores achieved on these standardized certification exams were not statistically different when comparing delivery modalities – such as whether the course instruction was taken via our traditional, live instructional format or via either our OnDemand or vLive instructional modalities....A similar analysis was conducted using calendar year 2014 exam outcomes. Results from the analysis were consistent with trends noticed in the 2013 study of all certification exams. On average, students who enrolled in a distance education course in 2014 performed slightly better on exams than students who enrolled in in-person courses.”

To update these assessments, the Working Group once again compared the GIAC scores of students who had taken their classes live versus those who took their classes through STI’s OnDemand modalities, and once again found the measured learning outcomes to be the same among both groups (Table A4.1).

**Table A4.1. Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017**

Modality	Overall Score	Master’s Program	Certificate Program
Live Class	84.6	86.6	82.4
OnDemand Class	83.7	87.2	82.0

**(iii) A program shall result in learning outcomes appropriate to the rigor and breadth of the program.**

The learning outcomes of the courses included in the Bachelor of Professional Studies in Applied Cybersecurity program have been validated by the faculty as appropriately rigorous and broad and are integrated into each course and measured quantitatively through ANSI-standardized certification exams for the three advanced courses and through integrated testing in each of the other courses.



**(iv) A program shall provide for appropriate real-time or delayed interaction between faculty and students.**

A teaching assistant referred to as a virtual mentor is available for all OnDemand courses to help answer student questions or assist with lab issues.

The vLive learning modality is conducted online with established course meeting times led by an instructor – typically twice per week for up to eight weeks – through a learning management system that allows for direct interaction with the instructor and other course participants. Each course session is recorded for students to review previously covered material, or to view if they miss a session.

The Simulcast delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time that the in-person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

**(v) Faculty members in appropriate disciplines in collaboration with other institutional personnel shall participate in the design of courses offered through a distance education program.**

STI faculty members design all distance learning programs.

**(b) Role and mission**

**(i) A distance education program shall be consistent with the institution's mission.**

The distance education program at STI is identical in content and impact to the live training program and has been designed, with strong faculty leadership and deep embedded course and program assessment, to focus precisely on meeting STI's mission to develop leaders to strengthen enterprise and global information security.

**(ii) Review and approval processes shall ensure the appropriateness of the technology being used to meet a program's objectives.**

The appropriateness of the technology STI uses for distance education has evolved over more than 11 years to be optimized for meeting the active learning needs of full-time working professionals, and it has been assessed and approved by STI faculty. But that is not the end of the development process. The distance learning technology is continuously assessed through evaluations completed by every one of the more than 3,000 cybersecurity professionals using it each day. If a course is not helping students master the key learning objectives, we hear about it quickly and fix the problems.

### **(c) Faculty support**

**(i) An institution shall provide for training for faculty who teach with the use of technology in a distance education format, including training in the learning management system and the pedagogy of distance education.**

Faculty who participate in our OnDemand, vLive, and Simulcast distance learning modalities undergo specific training to help modify their style to this format. We engage a team of individuals to assist in online-specific methods to enable virtual student-faculty interactions, including (when a class is Simulcast to students) employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructor's attention when questions are asked or issues are raised by virtual students.

**(ii) Principles of best practice for teaching in a distance education format shall be developed and maintained by the faculty.**

Members of the STI faculty have developed guidelines for best practice when teaching in our distance education formats. The guidelines are reproduced below.

### ***Instructor Guidelines for SANS Simulcast Classes***

#### **What to Expect**

During a SANS Simulcast you will be teaching live students in the same room AND students at remote locations. To accomplish this, your on-site moderator will log into GoToTraining and our system will capture everything that is projected in the classroom. You will also wear a wireless microphone to transmit your voice to remote students. The moderator will also set up a webcam and broadcast video from the classroom. We highly encourage the use of video, but if you do not want video to run in your class, please contact the Simulcast staff.

All-day classes will be broken into two sessions: morning and afternoon. When you break for lunch please remind all students to log out of GoToTraining and to log into the afternoon session when they return. You will also need to do the same thing, so please return from your lunch break a few minutes early. The key to teaching a successful vLive! Simulcast is to always **remember that you are teaching remote students; keep them engaged** by promptly responding to their questions and periodically addressing them directly ("Before we move on, are there any questions from our remote students?").

#### **Advance Planning**

1. The vLive! and OnSite teams will schedule a planning call with the customer point of contacts two weeks before the course; please plan on attending this call.
2. The AV kit that contains all necessary equipment for the Simulcast will be shipped to the Simulcast location prior to class.
3. The vLive! support team will be setting up the audio equipment and test the setup with you. This test is critical to the success of the Simulcast session and must be completed prior to starting class.

4. If it is possible, plan to do the audio testing the day before class starts. If this is not possible please make sure you arrive 2 hours early on the first day of class to complete the audio setup.
5. The vLive! team will introduce you to the virtual moderator who will be working the classroom. This moderator is a SANS employee who is there to assist with running the Elluminate platform, running labs, and assisting with student questions. Many instructors prefer that the moderator relay questions from the virtual students by raising his or her hand and reading the question.

### Audio Tips

6. Do not wear your cell phone on your belt next to the transmitter or lay it next to the receiver by the laptop. Your cell phone and student cell phones can create interference. You may need to disable Bluetooth functionality on your phone if it is causing buzzing.
7. Leave your wireless microphone on at all times, but turn off your GoToTraining audio during breaks. To do this, simply ask your on-site moderator to mute you on the Simulcast laptop.
8. ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.

### Starting Class

9. When it is time to start class, your moderator will start the recording and give you a signal that everything is ready on the remote side.
10. After the moderator has turned the class over to you, introduce yourself and briefly explain to students how the Simulcast class will work.
11. It is important to make the remote and on-site students aware of each other. Identify and welcome each remote site by name. A roster with the remote sites and student counts will be provided to you.
12. Please encourage remote students to participate by typing their questions and comments into the Chat window.
13. Directing questions about class material to the virtual students can also help to keep them engaged throughout the class.
14. The moderator will relay any questions from the online students to you.
15. Discuss any other housekeeping items as needed (timing of breaks, confirming that VMWare is correctly set up, etc.).

### Teaching Tips

16. ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.
17. If you need to discuss issues that students should not see, please use the “Organizers Only” or “private message” chat option as your means of communication.
18. Address remote students often to ensure they feel like they are part of the class; remote students become passive listeners if they are not actively engaged.

19. All scripts, videos, demos, etc. that you wish to show to students must be shared with GoToTraining's application sharing feature.
20. Remote students' systems (and your host's network) can be slowed down if you send very large files. If a file is necessary for class try to send it before class or during a break. If it is not course-related (e.g., music while on break), consider not sending it.
21. Use the GoToTraining timer when breaking from lecture so remote students know when class will be resuming; tell the moderator how many minutes you would like and they will set up the timer for you.
22. When breaking for lunch, please explain to students that they will need to log out of the morning session and log into the afternoon session upon their return.
23. Allow plenty of time to log into GoToTraining when arriving in the morning or returning from lunch. Depending on the location, you may have to extend the lunch break.
24. Conduct a quick audio check after each break and lunch to confirm that your microphone is on and that your remote students can hear you.

### Suggested Best Practices

Jason Fossen (SANS Senior Instructor):

- Each day I used a second laptop to log onto vLive as an attendee so that I could see how fast my application sharing window was updating its screen.
- ◇ It was also useful for checking the sound, video, and file-sharing features.
- ◇ I granted my other account moderator status so that, in case my primary laptop had an issue, I could switch over to the secondary and continue teaching.
- New vLive instructors (or new laptops for prior instructors) should go through the setup and test process before flying on-site; there won't be enough time to fix any problems like these the morning of.
- Return early after lunch to log back into GoToTraining.
- Make sure your Internet connection is wired and not shared by the students.
- Make sure to have the vLive emergency contact info on hand.
- The instructor should have the slides to teach the course on his/her laptop in case the slides in the vLive system are missing, wrong, or have any problems.

Jason Lam (SANS Senior Instructor):

- Make sure that the OnSite students are aware of the virtual students.
- Be available for remote students before or after class in the Elluminate Office session.
- Depending on the class size and your teaching style, you might need longer than usual to prepare for class (questions, demos, labs).
- Have the moderator type names of products, vendors, URLs, etc. in the chat for the virtual students.

**(iii) An institution shall provide faculty support services specifically related to teaching through a distance education format.**

SANS Simulcasts are supported by the OnSite and vLive teams. The OnSite team takes the lead with most sales issues, while the vLive team provides most of the support during class.

**(d) An institution shall ensure that appropriate learning resources are available to students including appropriate and adequate library services and resources.**

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that helps STI students and alumni maintain their edge in security. The SANS Resource Center is a compilation of thousands of original research papers, security policies, and security notes, along with a wealth of unique network security data. The list below outlines some of the primary resources available.

- The SANS Information Security Reading Room contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year. The Reading Room is available at [http://www.sans.org/reading\\_room/](http://www.sans.org/reading_room/).
- The SANS Security Policy Collection contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Top-20 V7 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection helps keep students up to date with the high-level perspective of the latest security news.
- The Security Glossary is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at <http://www.sans.org/security-resources/idfaq/>.
- The SANS Internet Storm Center Archives contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms spread through the Internet.
- SANS Web Briefings held several times a month feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

**(e) Students and student services**

**(i) A distance education program shall provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.**

- Curriculum information is posted, in detail, on the SANS.EDU website at <https://www.sans.edu/academics/>
- Course and degree requirements are posted online in the STI Course Catalog at <https://www.sans.edu/downloads/STI-Course-Catalog-2018.pdf>
- The nature of faculty/student interaction is described on our website at <https://www.sans.edu/academics/course-delivery/more>
- Assumptions about technology competence and skills are posted on our Admissions website at <https://www.sans.edu/admissions/masters-programs>
- Technical equipment requirements are posted with individual courses on the SANS course website. For example, for ACS 3504: Incident Handling and Hacker Exploits, the corresponding course site at SANS (<https://www.sans.org/course/hacker-techniques-exploits-incident-handling>) provides detailed technical requirements as well as a tech support contact to help students ensure they have the right equipment and software versions.
- Learning management systems information is posted in detail at <https://www.sans.org/ondemand/faq>
- The availability of academic support services and financial aid resources is posted at <https://www.sans.edu/students/services>, and on page 33 of the Student Handbook at <https://www.sans.edu/downloads/sti-student-handbook.pdf>
- Costs and payment policies are posted at <https://www.sans.edu/admissions/tuition>

**(ii) Enrolled students shall have reasonable and adequate access to the range of student services to support their distance education activities.**

With STI students taking approximately half of their credits through distance learning, the overall satisfaction with student services may be considered a reliable surrogate for effectiveness of distance learning student services. Evidence from student surveys indicates that measures of overall student satisfaction are high (above 90%)/. Quantified measures of specific sub-processes with student management were also high, with about 90% of respondents saying they were “Somewhat Satisfied” and “Very Satisfied” for each of the operational elements (Table A4.2).

**Table A4.2. Student Satisfaction with Student Management as Reported in the 2016 Student Experience Survey**

	<b>Very Dissatisfied</b>	<b>Somewhat Dissatisfied</b>	<b>Somewhat Satisfied</b>	<b>Very Satisfied</b>
Registration/Billing	<1%	10%	21%	68%
Academic Advising	2%	8%	25%	65%
GI Bill Certification	2%	6%	17%	75%

**(iii) Accepted students shall have the background, knowledge, and technical skills needed to undertake a distance education program.**

Our BACS students will be upper division students, likely at least 19 years old, and sufficiently well versed in information technology to have scored sufficiently high on the cyber aptitude test and simulator gain acceptance. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

**(iv) Advertising, recruiting, and admissions materials shall clearly and accurately represent the program, and the services available**

Advertising, recruiting, and admissions materials for BACS students are currently being drafted. STI has a solid record of meeting Middle States' high standards for transparency and accuracy in all its marketing and admissions materials and will continue to do so.

**(f) Commitment to support**

**(i) Policies for faculty evaluation shall include appropriate consideration of teaching and scholarly activities related to distance education programs.**

Every teacher is evaluated every day by every student, and those evaluations specifically measure the teachers' effectiveness in distance education. Those evaluations affect teachers' compensation as well as their long-term career prospects with STI.

**(ii) An institution shall demonstrate a commitment to ongoing support, both financial and technical, and to continuation of a program for a period sufficient to enable students to complete a degree or certificate.**

STI has adequate faculty, infrastructure, and financial resources, as demonstrated in Sections H, J, and K, to implement the new BACS program. Further, because the undergraduate program is core to our mission and was specifically discussed during the Middle States 2018 Team Visit as a critical step for meeting that mission, we have demonstrated both the commitment and resources to maintain the program for many years.

**(g) Evaluation and assessment**

**(i) An institution shall evaluate a distance education program’s educational effectiveness, including assessments of student learning outcomes, student retention, student and faculty satisfaction, and cost-effectiveness.**

STI employs a three-level evaluation program completely embedded in the curriculum. The 2018 Middle States Evaluation Team commended this evaluation methodology: “SANS Technology Institute should be commended for the fact that its curriculum automatically embraces learning outcomes and program outcomes.” The assessment system and processes are detailed in Section M. This same system will be used in the distance learning component of the proposed BACS program

**(ii) An institution shall demonstrate an evidence-based approach to best online teaching practices.**

STI online teaching practices are currently in use by more than 3,000 students, and at least 50,000 students have used it during the past eight years. Each of those students evaluates the effectiveness of the learning modality in every course, and we continually improve the practices to ensure those ratings continue to match or exceed live classroom training scores.

**(iii) An institution shall provide for assessment and documentation of student achievement of learning outcomes in a distance education program.**

Ultimate student achievement in the BACS program will be measured by grades on the internationally standardized GIAC exams for each area of security. We compare these scores in distance and in-person learning modalities. As shown in Table A4.3, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

**Table A4.3. Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017**

<b>Modality</b>	<b>Overall Score</b>	<b>Master’s Program</b>	<b>Certificate Program</b>
Live Class	84.6	86.6	82.4
OnDemand Class	83.7	87.2	82.0

We will continue to monitor GIAC scores in the BACS program, by delivery modality.